SysMaster GW 7000 Digital Gateway

User Manual

version 1.0

Printed in the United States of America.

Contents

Chapter 15 Appendix A

What is New

Version 02.0.47

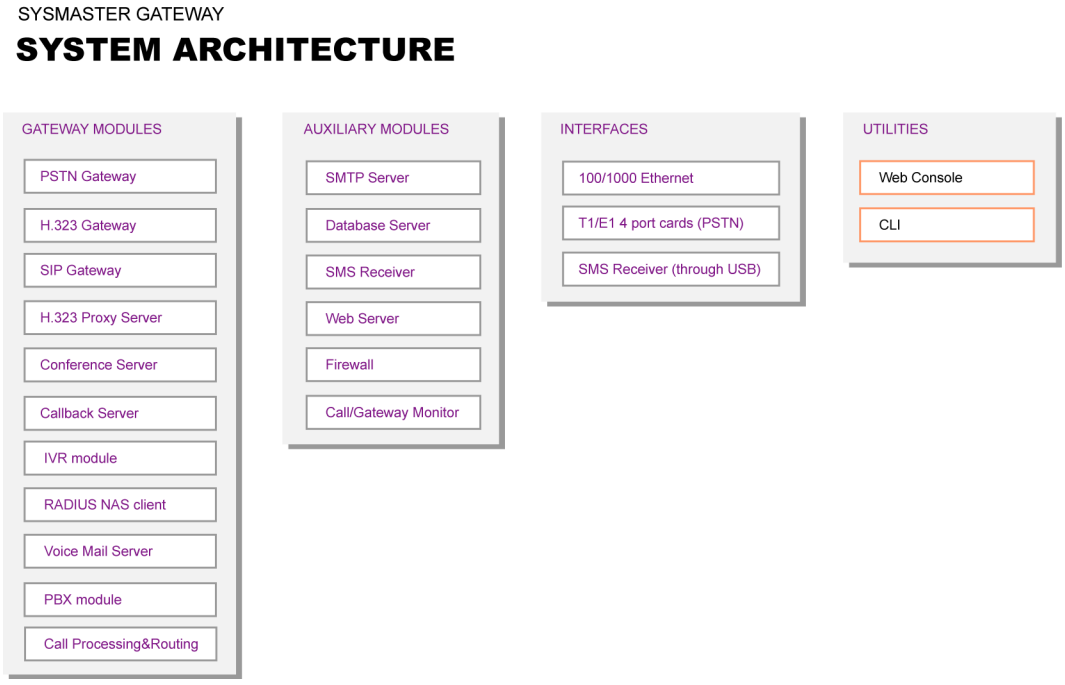
1. SIP GW: New “Domain Name” field in Endpoints for SIP Gateways. To be used in To/ Register URI
2. SIP GW - Prevents sending empty quoted string (“”) in name-addr (From) field as some implementations do not decode it
3. SIP GW - Receive info digits (ANI-II)

Version 02.0.46

1. SIP GW: Ability to configure User Agent in System Configuration > SIP User Agent
2. SIP GW: Refuse incoming initial requests with To tag and return reason code 481
3. SIP GW: Encode message-summary body by using CRLF instead of LF
4. SIP Proxy: Forward body in NOTIFY
5. SIP Proxy: Do not set ports in From/To field
6. SIP Proxy: When changing Host in Contact the Port field will also be changed for most request/response methods
7. SIP Proxy: Use “Expires: 0” for unsubscribe
8. SS7/MTP3: Signaling Points: State information, estimators
9. SS7/ISUP: Circuit Groups: State information, estimators
10. SS7/ISUP: Add “Called Party NOA” to Outbound Profile to allow changing the Nature of Address Indicator in outgoing calls
11. SS7/ISUP: Add “FCI Call Type” to Outbound Profile to allow selecting between national and international outgoing calls in Forward Call Indicators
12. PSTN: Busy detection for FXS signaling

Chapter 1 System Setup

System Architecture



Licensing

The SysMaster gateway is built by modules. This allows for flexible adding of different functionalities over time. You can view the currently installed modules by browsing the Navigator tree to **System Management > Licensed Modules**.

In the right pane of the Navigator you will see:

Module	Full name of the module.
ID	Coded short name.
Status	Displays the current status of the module and the date when it will expire.
Description	Designated the name of the provider. The name could contain any combination of numerical and alphabetical characters.

Using the Navigator tree - **System Management > Licensed Strings**. In the right pane of the Navigator you will see the license string of the gateway.

General System Settings

Overview

Parameters:

Gateway ID	Specifies the Gateway ID. The Gateway ID could be entered as either numerical or alphabetical value.
Domain Name	Refers to the group name assigned to all computers and network devices present on a company's network. A company's domain name is usually in the form of <companyName>.com
Host Name	Defines the host name of the device. The host name is the name used in identifying the device on a network and is combined together with the domain name to form the Internet address of the SysMaster device. The host name could be comprised of any combination of alphabetical and numerical characters in tandem with underscore, hyphen or dot notations.
NTP Server	Refers to the Network Time Protocol (NTP) Server designed to synchronize computer clocks over a network. The time synchronization is conducted on hourly bases based on the time of the specified NTP Server.
Time Zone	By default SysMaster operates in the Universal Time Coordinated (UTC) zone or Greenwich Mean Time (GMT) (same as UTC). In order for the management company to change the default time zone, a different one should be selected.

DNS Server 1	Defines the DNS Server used on a gateway level by the system for resolving computer Internet names. In the processes Internet domain and host names are translated to IP addresses. There could be up to two DNS Servers defined by having there respective IP addresses specified. The IP address should be entered as x.x.x.x notation, where x denotes a number from 0 to 255. The proper DNS setup enables the system to perform upgrades over the Internet.
DNS Server 2	Defines the second DNS Server used on a gateway level by the system for resolving computer Internet names. In the processes Internet domain and host names are translated to IP addresses. There could be up to two DNS Servers defined by having there respective IP addresses specified. The IP address should be entered as x.x.x.x notation, where x denotes a number from 0 to 255. address of the URL.
Backup Interval	Specifies how often a backup of the gateway database should be performed.

Managing General System Settings

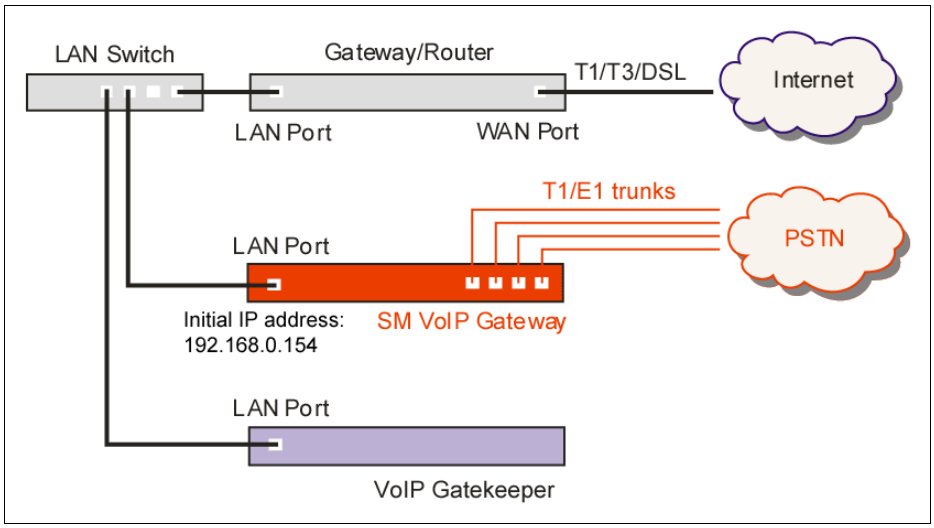
To Edit General System Settings

1. From the Navigation tree, select the **System Management > System Configuration** node.
2. From the right pane of the Navigator, select the first table entry.
3. From the Navigator menu, select 'Edit Settings'.
   A dialog will show up.
4. Fill in the data and click on the Apply button to enforce the settings. The settings take effect immediately.

Network Settings

Network Configuration

A Network Configuration specifies an IP address together with network within which the gateway is deployed. It includes additional parameters to provide information about the networks in which the gateway resides.



Network Configuration Parameters:

Local IP Address	Assigns the local IP address of the network. The local IP address will define the Local Network and servers (mail server, web server, etc.) on the network could "listen" to the local IP address defined.
Network Device	Specifies the network device. All hosts within the established Local Network would be available on the network device selected. Available choices are: eth0 eth1
Visibility: Public / Private	Determines the state of visibility of the Local Network. Public visibility indicates that the defined Local IP Address could be accessible via remote hosts located on remote gateways. Private visibility indicates that the Local IP Address would be accessible only through IP addresses located in the Local Network). When the latter scenario is present no gateways are necessary for routing to take place.
Web Access	Allows an access to the Web interface from remote locations using this IP address and network device.
SSH Access	Allows a Secure Shell (SSH) access through the specified IP address and network device. Secure Shell allows a secure remote administration of the device to be performed.

Managing Network Configurations

To Add Network Configuration

1. From the Navigation tree, select the **System Configuration > Network Configuration** node.
2. From the Edit Menu select 'Add Network Configuration'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to complete the operation.

To Edit Network Configuration

1. From the Navigation tree, select the **System Configuration > Network Configuration** node.
2. From the right pane of the Navigator, select the Network Configuration to be edited.
3. From the Edit Menu select 'Edit Network Configuration'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to complete the operation.

To Delete Network Configuration

1. From the Navigation tree, select the **System Configuration > Network Configuration** node.
2. From the right pane of the Navigator, select the Network Configuration to be deleted.
3. From the Navigator menu select the 'Delete Network Configuration' to complete the deletion.

Network Routes

Network Routes are used in accordance to their relevance to the target network. For example, network routes are sorted in descending order as far as the target network is concerned. Thus, the first route to be used would be /32 (host route) and the last one 0.0.0.0/0.

Network routes do not use default IP addresses. Network routes select the IP address to be used based on the Gateway and network device assigned to the route.

Route Parameters:

Destination Network	Specifies the target host that the route could be traced to. The destination network (target host) could be assigned as either host route (IP/32) or a network route (IP/24).
Gateway	Specifies the IP address of the gateway participating in the route. The IP address specified could be either public or private one. If private IP address is present the gateway would participate in direct routing.

Network Device	Specifies the network device responsible for sending traffic from the target network to the host network. Available choices are: eth0 eth1
Status	Indicates whether the network route is activated or not.

Managing Network Routes

To Add Network Route

1. From the Navigation tree, select the **System Configuration > Network Routes** node.
2. From the Edit Menu select 'Add Network Route'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to complete the operation.

To Edit Network Configuration

1. From the Navigation tree, select the **System Configuration > Network Routes** node.
2. From the right pane of the Navigator, select the Network Route to be edited.
3. From the Edit Menu select 'Edit Network Route'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to complete the operation.

To Delete Network Configuration

1. From the Navigation tree, select the **System Configuration > Network Route** node.
2. From the right pane of the Navigator, select the Network Route to be deleted.
3. From the Navigator menu select the 'Delete Network Route' to complete the deletion.

Firewall Settings

Overview

SysMaster gateway comes with an integrated Firewall. The task of the firewall is to restrict the access to the server from the Internet for security reasons. It can also be used to eliminate some of the common TCP/IP based attacks.

Parameters:

Source IP Network	Specifies the source IP network from which packets would be transported.

Destination IP Network	Specifies whether packets should be sent to the specified destination formed by the Destination IP Network, network bits and port in order to match the rule.
Action	Specifies the action of the firewall filter. Available options are: ■ Disabled - a firewall filter cannot be applied to packets. ■ Allow - packets will be processed. ■ Reject - packets will not be processed an error message will be sent in response. ■ Drop - packets matching the firewall filter parameters would be ignored.
Protocol	Specifies whether a specific protocol should be used in determining which packets of data can or cannot transport information.
Direction	Specifies whether the firewall filter will be applied on inbound or outbound packets.

Managing Firewall Filters

To Add Firewall Filter

1. From the Navigation tree, select the **System Configuration > Firewall Filter** node.
2. From the Edit Menu select 'Add Firewall Filter'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to complete the operation.

To Edit Firewall Filter

1. From the Navigation tree, select the **System Configuration > Firewall Filter** node.
2. From the right pane of the Navigator, select the Firewall Filter to be edited.
3. From the Edit Menu select 'Edit Firewall Filter'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to complete the operation.

To Delete Firewall Filter

1. From the Navigation tree, select the **System Configuration > Firewall Filter** node.
2. From the right pane of the Navigator, select the Firewall Filter to be deleted.
3. From the Navigator menu select the 'Delete Firewall Filter' to complete the deletion.

System Users

Overview

System users are required so that the access to the administration console is controlled and managed. Each user needing access to the administration console should have a system user account. The system supports three levels of resource access and privileges enforced through roles:

- Admin role - Grants full privileges to access and modify any resource, with the exception of accessing voicemail audio files of regular PBX users;
- Guest role - Grants only viewing privileges similar to those of an administrator.
- User role - Grants privileges of PBX users to view their respective voicemail boxes and listen/delete voicemail messages (files).
- Conference PBX role - Grants full privileges to Conference PBX users.
- Follow-Me role - Grants full privileges to Follow-Me users.
- VoiceMail role - Grants full privileges to VoiceMail users.

Parameters:

Login Name	Specifies the login name of the user. The login name is used for authentication of users and in determining their administrative functions in front of the system. The login name is entered in the form of a string that could be combined by either numerical or alphabetical (or both) characters.
Password	Specifies the password of the user. The password, together with login name are used in the process of user authentication and authorization. Passwords should be safeguarded. For safety reasons, it is highly recommended that passwords are as complex as possible and changed on frequent basis. Please, consider the following options when choosing a user password: It is advisable that your password should: ■ Contain between 8 and 14 characters ■ Contain both lowercase and uppercase alphabetical characters in addition to numbers ■ Not appear in any dictionary ■ Contain non-alphabetical characters such as !, @, #, $, %, ^, &, *, etc
Confirm Password	Requires that the password previously entered be confirmed.
Full Name	Designates the name of the account holder.

Role	Determines the role of the user to be assigned. The following user roles are available: ■ Admin ■ VoiceMail User ■ PBX User ■ VoiceMail/PBX User

Managing System Users

To Add System User

1. From the Navigation tree, select the **System Configuration > System User** node.
2. From the Edit Menu select 'Add System User'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to complete the operation.

To Edit System User

1. From the Navigation tree, select the **System Configuration > System User** node.
2. From the right pane of the Navigator, select the System User to be edited.
3. From the Edit Menu select 'Edit System User'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to complete the operation.

To Delete System User

1. From the Navigation tree, select the **System Configuration > System User** node.
2. From the right pane of the Navigator, select the System User to be deleted.
3. From the Navigator menu select the 'Delete System User' to complete the deletion.

Upgrades

Overview

SysMaster Gateway provides an upgrade functionality. It allows administrators to upgrade the SysMaster gateway to the latest version. The system allows only for upgrades. Downgrading is not allowed.

Performing Upgrades

The upgrade procedure can be performed only by system users having an administrative privileges (through the admin role). The procedure includes 2 steps:

1. **Refresh the Upgrade List**
   This action makes the SysMaster gateway contact the sysmaster.com site and checks for newer versions available for upgrade. In order for this functionality to work, please

make sure the SysMaster has correctly set a Network Gateway (to provide access to the Internet) and a DNS server and that generally it has access to the Internet. The status of the available for download upgrades is “not downloaded“.

2 **Download the Upgrade file**
This action selectively downloads the required upgrade. After download it is ready to be installed. The downloaded upgrade is stored internally on the SysMaster gateway. The downloaded upgrade has a status “not installed“.

3 **Install the Upgrade File**
This action applies a selected upgrade to the SysMaster gateway. The installed upgrade has status “installed“.

NOTE: The system does not support downgrade.

To Refresh the Upgrade List

1 From the Navigation tree, select the **System Configuration > Upgrades** node.

2 From the Edit Menu, select ‘Refresh Upgrade List’.

3 The SysMaster gateway contacts the sysmaster.com web site and lists all upgrades available for download.

To Download the Upgrade File

1 From the Navigation tree, select the **System Configuration > Upgrades** node.

2 From the list on the right pane of the Navigator, select the upgrade to be installed

3 From the Edit Menu, select ‘Download Upgrade’.

4 The SysMaster gateway will download and store the upgrade files internally.

To Install the Upgrade to the System

1 From the Navigation tree, select the **System Configuration > Upgrades** node.

2 From the list on the right pane of the Navigator, select the upgrade to be installed.

3 From the Edit Menu select ‘Upgrade System’.

4 The SysMaster gateway will perform the upgrade and the SysMaster gateway will have to be restarted.

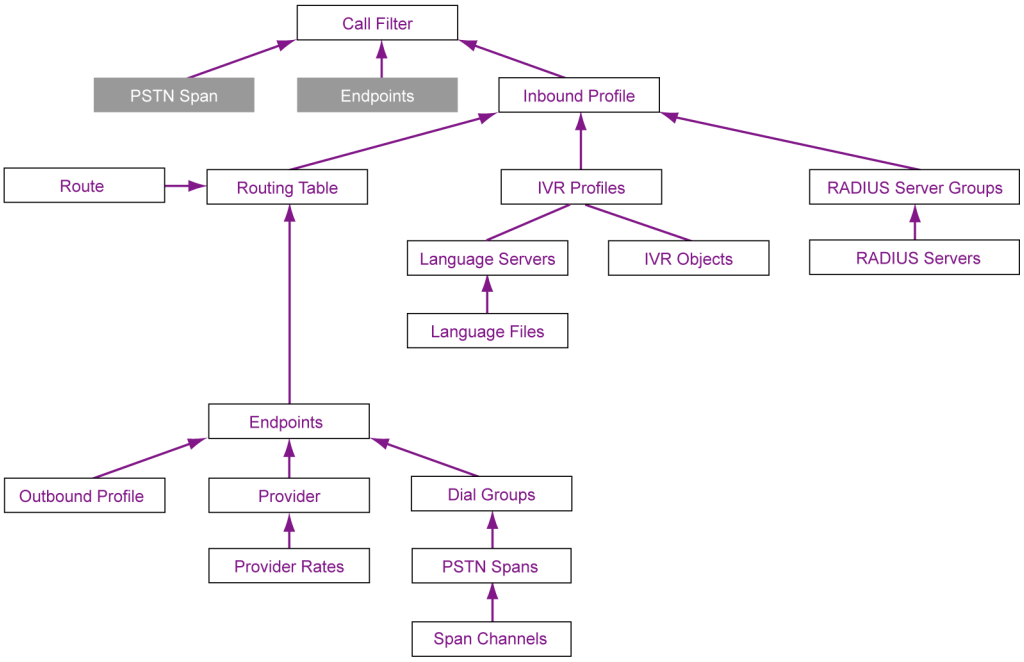
System Setup Workflow

Overview

The order of administration and setup of the SysMaster gateway is closely related to the way the system objects and resources are allocated and the way they interact between themselves. Below is a diagram illustrating the system object dependencies.

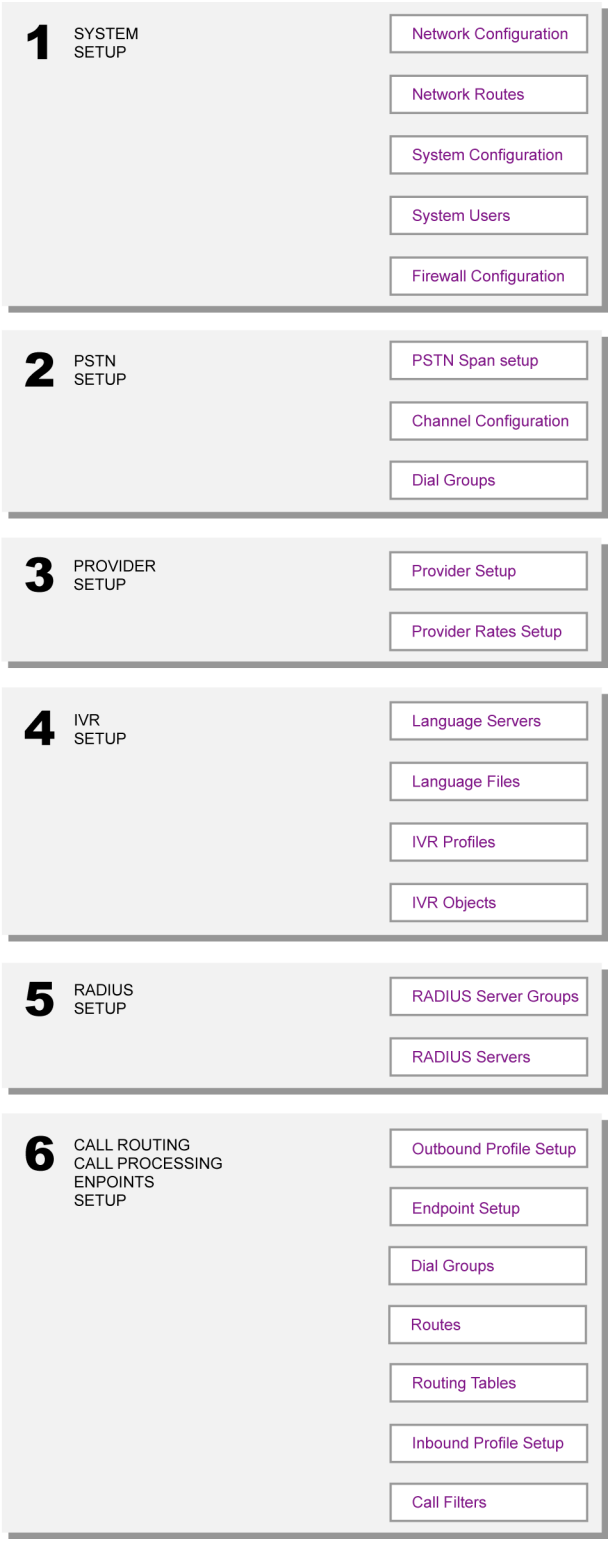
SYSMASTER GATEWAY

OBJECT DEPENDENCIES



SYSMASTER GATEWAY

SETUP WORKFLOW



The Setup workflow diagram shows the steps for setting up the SysMaster gateway. It outlines 6 steps:

1. **System Setup**
   This section covers all basic functionality necessary for operating the gateway. It deals with TCP/IP networking, Upgrading, System Users, Firewall filters
2. **PSTN Setup**
   The PSTN Setup phase deals with configuring the PSTN spans and channel parameters. PSTN Spans are used in call filters to catch PSTN originated traffic. Span/channels is used in defining Dial Groups.
3. **Provider Setup**
   Provider Setup deals with setting up providers as well assigning Provider rates for the purposes of implementing Least Cost Routing algorithms when the gateway choses from among multiple endpoints, belonging to different providers, to route the call. Providers are attached to endpoints.
4. **IVR Setup**
   IVR is dependent on Language servers/ Language Server files. In addition, for the purposes of the PBX, there could be built custom audio menus that rely on IVR Objects. IVR functionality works in tight relationship with RADIUS communication. IVR functionality is optional.
5. **RADIUS Setup**
   RADIUS setup includes defining first RADIUS group and then RADIUS servers for the respective group. RADIUS servers are not always required - depending on the mode in which the gateway works. E.g. in H.323 proxy mode, RADIUS servers are optional.
6. **Call Routing, Call Processing, Endpoints Setup**
   At this last stage of the system setup, administrators can build the main logic for processing calls.

   Endpoints setup includes the definition of all gateways, gatekeepers, dial groups etc endpoints with which the gateway will communicate. Use Dial Groups (through Endpoint definitions) to terminate calls to PSTN and Spans (in Call Filters) to capture calls from the PSTN.

   Call Routing requires to first create routing tables and then populate them with routes. Each route is a pair of area code and endpoint.

   Call Processing parameters like Inbound Profiles are policies for aggreagited processing instructions imposed on prefiltered calls. The process of call filtering is done on the level of Call Filters. Outbound Profiles include call manipulation behavior imposed right before the call “leaves“ the gateway.

The above described Setup workflow is suitable for setting up any operational mode of the gateway.

Other System Management Tasks

Overview

The console allows administrators to perform the following commands on some of the basic servers running on the gateway:

- Restart VoIP Gateway

- Restart SMS Server - related to SysMaster Callback server
- Restart DataBase Server - highly undesirable actions
- Restart Mail Server - related to SysMaster Callback server
- Restart All Servers
- Restart SysMaster Device - restarts all servers
- Halt SysMaster Device - stops all servers.
- Restore Database - this command will restore the database from the most recent database backup. Administrators can setup the frequency at which the databases performs backup of its data through the System Configuration dialog.

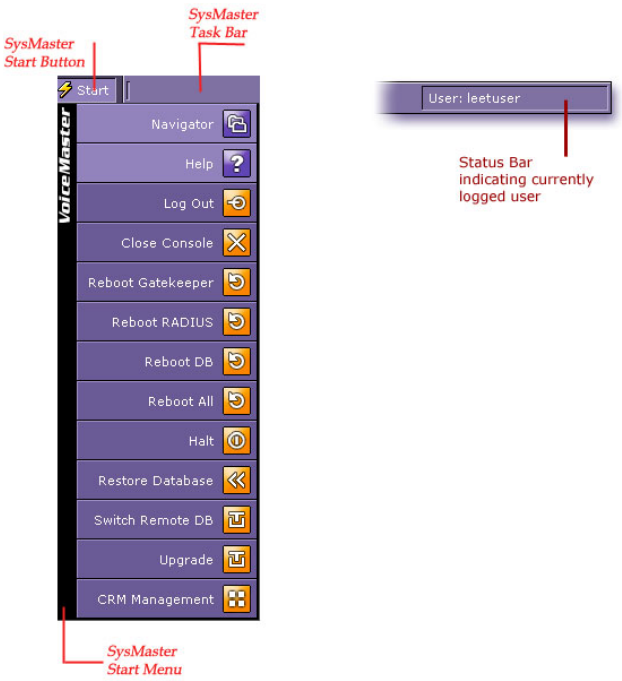
All of these commands can be reached from the Start menu of the console.

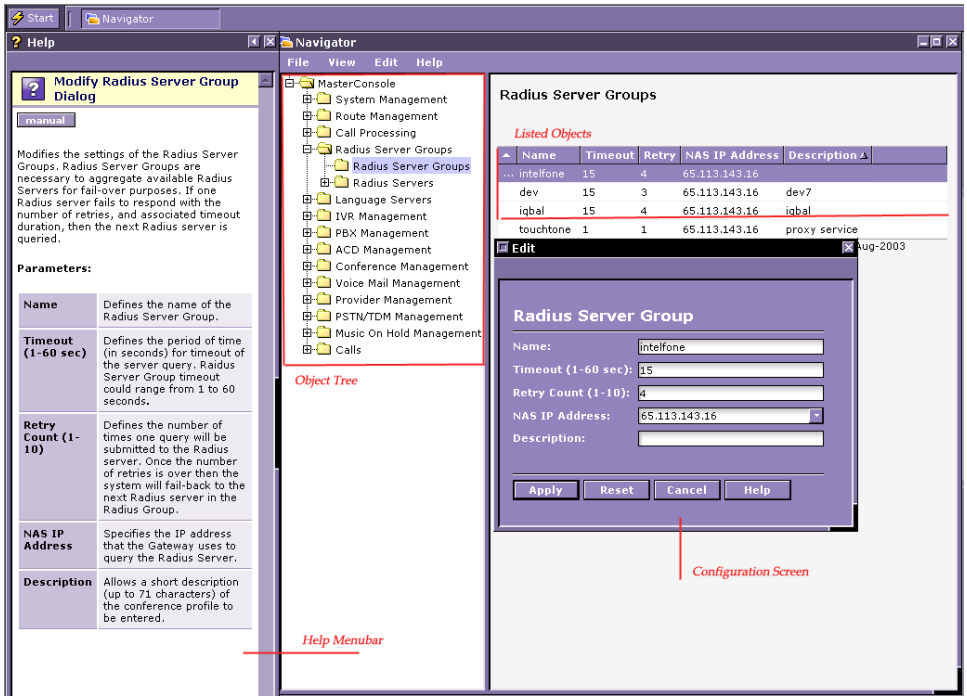
IMPORTANT: Please, be careful when restarting any server!

Chapter 2 Web Console Navigation

SysMaster Web Console Client features a web-driven, browser-based intuitive and powerful interface. The console interacts with the SysMaster administration web server for managing the system in a client-server fashion. When starting the console, a login prompt window will show up. A valid username and password should be provided. Usernames and passwords are case sensitive. The system allows for only one user to login with a given system user account at a time. The user is allowed to perform operations according to the privileges assigned by the administrator.

Web Console Components





1. **Start Button** – start point for running the Navigator window, show the Help window, Log out or close the console;
2. **Task Bar** – hosts all buttons hooked to opened windows of the application;
3. **Start Menu** – Contains basic commands for starting a new Navigator window, show the Help window, Log out and Close the console;
4. **Status Bar** – Displays the currently logged user in the system;
5. **Help Window** – Displays general help information or context information;
6. **Navigator Window** – Serves as a browser of system objects for setup of the system;

All windows can be:

- **Moved** - drag them using the title bar;
- **Minimized** – use the minimize button on the window title bar;
- **Maximized** – use the maximize button on the window title bar;
- **Closed** – use the close button on the window title bar.

The menu system on a Navigator Window contains the following commands:

- **File**
  - **New** – Opens a new Navigator Window;

- **Print** – Prints the contents of the right pane of the Navigator window;
- **Close** – Closes the window;

- **View**
  - **Refresh** – Refreshes the right pane of the Navigator window;
- **Edit**
  The Edit menu is dynamically changed, based on the selected object type from the tree. It always offers commands that are relevant to the currently selected object.
  - **Add** – Adds a new object;
  - **Modify** – Modifies an object selected in the right pane of the Navigator window;
  - **Delete** – Deletes an object selected in the right pane of the Navigator window;
- **Help**
  - **Contents** – Displays the Help window;
  - **About Us** – Shows the current version of the product;

Browsing and Managing Objects

The SysMaster Web Console features a Navigator window for browsing through the system objects and settings.

To open the Navigator window:

1. Use **Start Button > Navigator**;
2. Use the tree in the left pane of the Navigator window to browse through the objects and settings. With SysMaster every object can be listed in the right pane of the Navigator;
3. Click on a selected object from the tree;
4. On the right pane there will be listed all objects in the system relating to the object type selected in the tree;
5. Select an object to modify or delete;
6. Use the menu commands of the Navigator window. Alternatively, use the ellipsis button … or double click on the selected object to edit its definition.

Chapter 3 Call Processing

Call Flow

PSTN to PSTN Calls

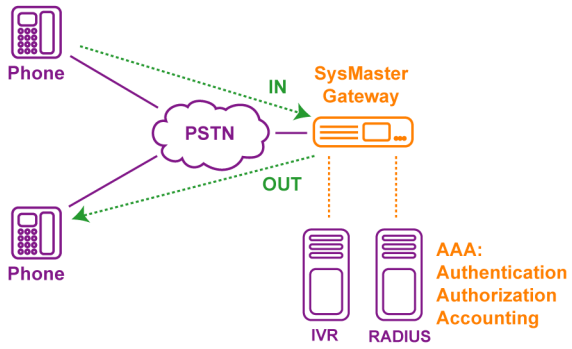
All call processing is done based on the diagram entitle "Call Flow - PSTN-to-PSTN, PSTN-to-VoIP"

In this setup there could be two cases:

1. The gateway detects that the call is to be routed back through PSTN
2. The gatekeeper, based on its routing tables, decides the call should be terminated by the same origination gateway i.e. be terminated in the PSTN

Case 1

PSTN to PSTN



1. The user dials into the gateway.
2. The call filter catches the call based on ANI, DNIS, or selected Span.
3. Next the gateway processes the call based on the selected Inbound Profile.
4. The gateway performs IVR processing according to the IVR Profile as indicated by the selected Inbound Profile.
5. The gateway performs RADIUS authentication according to the selected RADIUS Server group. This is indicated in the Inbound Profile.

6 The calling party is authenticated

7 The calling party provides destination number

8 RADIUS authorization is performed

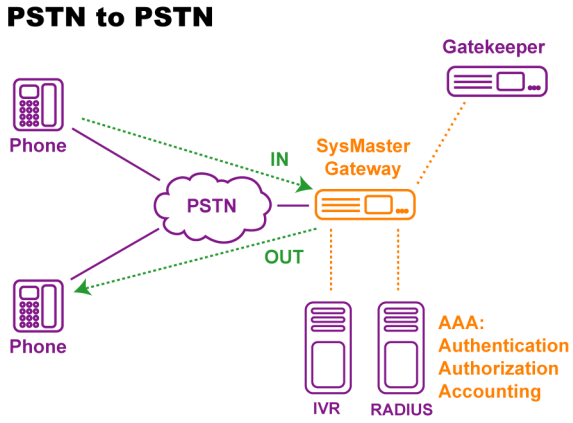
9 The gateway matches the destination number against the routing table selected by the Inbound Profile.

10 The area code selected points to an endpoint containing a dialing group that on its part contains PSTN span channels

11 The gateway tries to connect to the destination through the PSTN span/channels as specified in the dialing group.

12 Upon call disconnect, the gateway sends accounting message to the RADIUS server chosen from the selected RADIUS server group.

Case 2



1 The user dials into the gateway.

2 The call filter catches the call based on ANI, DNIS, or selected Span.

3 Next the gateway processes the call based on the selected Inbound Profile.

4 The gateway performs IVR processing according to the IVR Profile as indicated by the selected Inbound Profile.

5 The gateway performs RADIUS authentication according to the selected RADIUS Server group. This is indicated in the Inbound Profile.

6 The calling party is authenticated

7 The calling party provides destination number

8 RADIUS authorization is performed

9 The gateway matches the destination number against the routing table selected by the Inbound Profile.

10 The area code selected, points to a gatekeeper

11 RAS signalling to the gatekeeper is initiated. The Gateway should be registered with the Gatekeeper before they can communicate with each other.

12 The gatekeeper finds in its routing tables that this call should be terminated by the origination gateway.

13 The gateway creates an incoming call as if coming from its gatekeeper.

14 A second call filter catches the call through an Endpoint filter (there should be the local gatekeeper selected)

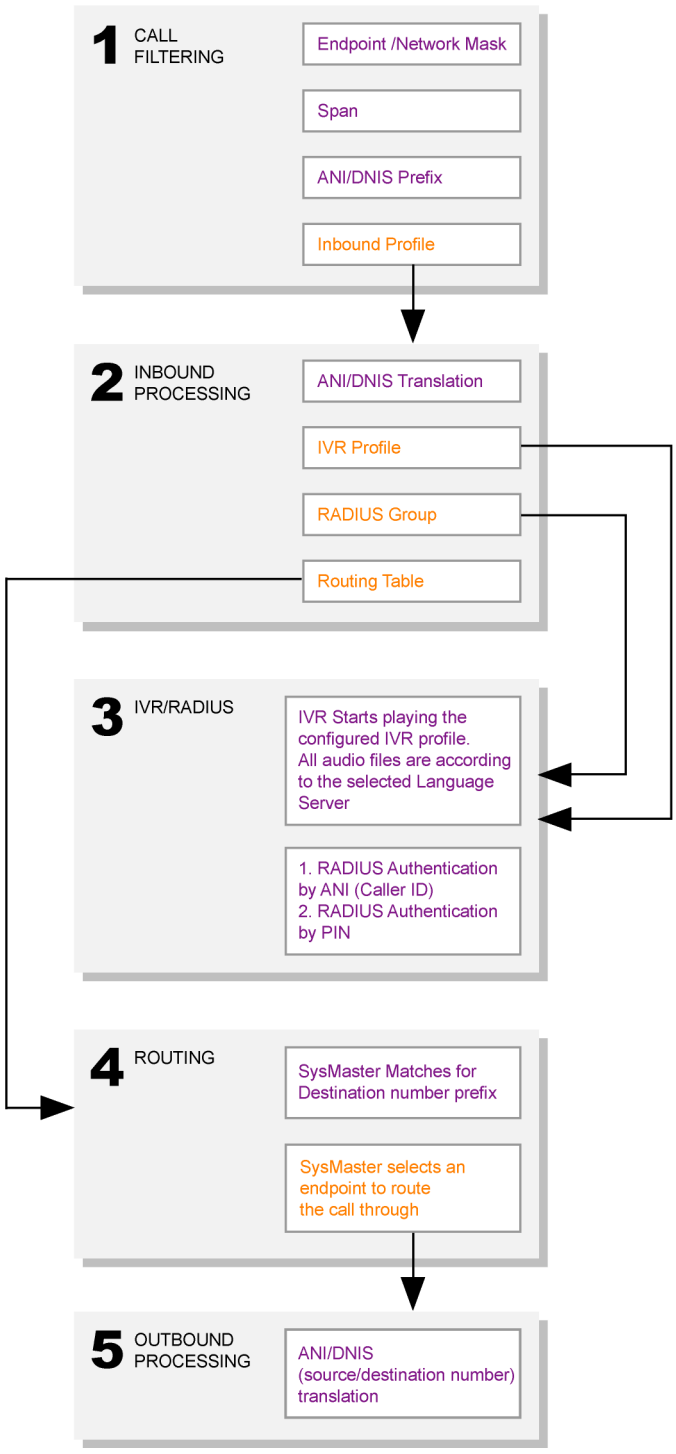
15 The Inbound Profile should point to an IVR Profile with CDR only policy, no RADIUS Server group, and Routing Table pointing to PSTN (i.e. Endpoint of type Dial Group).

16 The call is routed to a PSTN span/channel from the selected Dial Group.

17 Connection is established to the remote PSTN peer.

18 Upon call disconnect, the gateway sends accounting CDR message to the RADIUS server (chosen from the selected RADIUS server group of the first Call Filter/Inbound Profile).

Call Flow
PSTN to PSTN
PSTN to VoIP

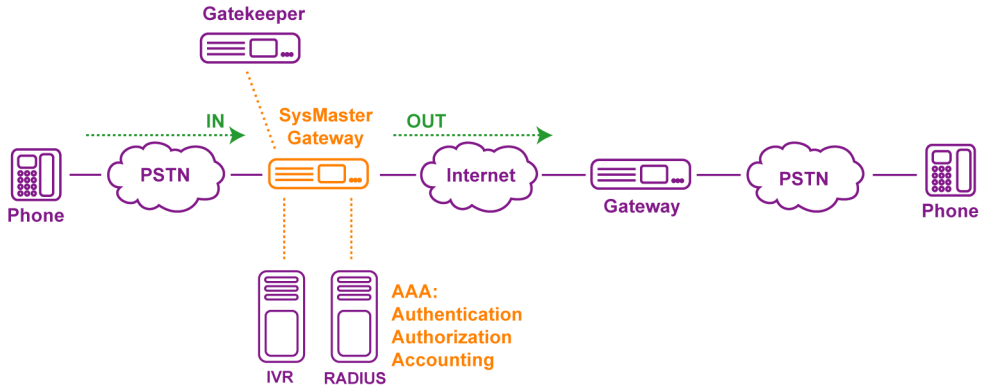


PSTN to VoIP Calls

All call processing is done based on the diagram entitle “Call Flow - PSTN-to-PSTN, PSTN-to-VoIP”.

This is a standard setup for VoIP calls.

PSTN to VoIP



1. The user dials into the gateway.
2. The call filter catches the call based on ANI, DNIS, or selected Span.
3. Next the gateway processes the call based on the selected Inbound Profile.
4. The gateway performs IVR processing according to the IVR Profile as indicated by the selected Inbound Profile.
5. The gateway performs RADIUS authentication according to the selected RADIUS Server group. This is indicated in the Inbound Profile.
6. The calling party is authenticated.
7. The calling party provides destination number.
8. RADIUS authorization is performed.
9. The gateway matches the destination number against the routing table selected by the Inbound Profile.
10. The area code selected, points to a gatekeeper
11. RAS signalling to the gatekeeper is initiated. The Gateway should be registered with the Gatekeeper before they can communicate with each other.
12. The gatekeeper finds in its routing tables that this call should be terminated by a termination gateway.
13. The gatekeeper returns to the Origination Gateway the IP address of the termination gateway in an ACF message (as part of the RAS signaling).
14. The gateway initiates a call setup to the remote gateway H.323 peer.
15. The termination gateway connects to the destination number through PSTN.

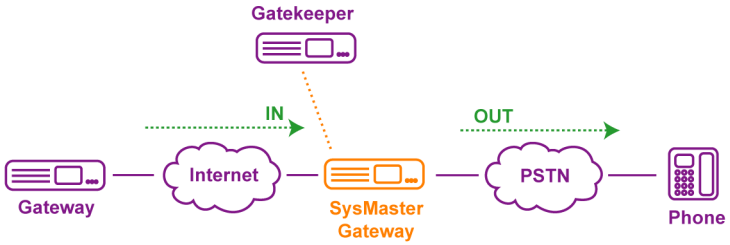
16 The connection between both ends is established

17 After call is disconnected, the gateway sends accounting message to the RADIUS with CDR records of the call.

VoIP to PSTN calls

This setup is relevant when the gateway is a termination endpoint. This is the case when other parties want to terminate calls to area codes serviced by the gateway through PSTN.

VoIP to PSTN



1 An incoming call request is received into the Sysmaster gateway.

2 The call filter catches the call based on source number prefixes or by endpoint.

3 The Gateway selects the Incoming Profile as indicated in the call filter.

4 The IVR profile should be CDR Only indicating no audio services are provided.

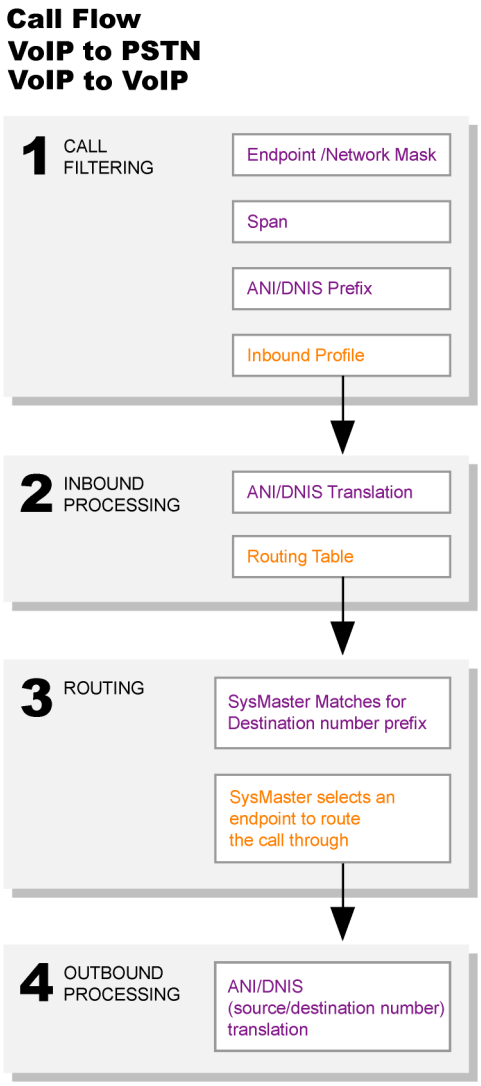
5 The RADIUS server selected will be used only for accounting purposes.

6 The gateway checks the selected Routing Table and selects a Dial Group Endpoint

7 SysMaster gateway select channels to connect through the PSTN.

8 The gateway connects to the destination number.

9 Upon call disconnect, the gateway sends accounting message to the RADIUS server and sends CDR data for the call.



VoIP to VoIP calls

There are three cases possible for this setup:

- **Case A**. IVR/RADIUS over IP
- **Case B**. H.323 Proxy Mode
- **Case C**. Termination to VoIP phone or VoIP software PC client

Case A. IVR/RADIUS over IP

In this scenario, there is a phone connecting to analog gateway. The gateway does not have neither gatekeeper, nor IVR server to contact, nor RADIUS server for AAA. The analog

gateway acts like a transparent proxy between the end user and the gateway. This scenario allows for building a cheap infrastructure across large areas with low volume of calls.

1. The user dials into the analog gateway.
2. The analog gateway contacts the main SysMaster digital gateway over the Internet.
3. An incoming call request is received into the Sysmaster gateway.
4. Next the gateway processes the call based on the selected Inbound Profile.
5. The gateway performs IVR processing according to the IVR Profile as indicated by the selected Inbound Profile. All IVR messages are sent over IP and are played by the analog gateway to the user.
6. The gateway performs RADIUS authentication according to the selected RADIUS Server group. This is indicated in the Inbound Profile.
7. The calling party is authenticated based on PIN.
8. The calling party provides destination number.
9. RADIUS authorization is performed.
10. The gateway matches the destination number against the routing table selected by the Inbound Profile.
11. The selected area code points to a gatekeeper
12. RAS signalling to the gatekeeper is initiated. The Gateway should be registered with the Gatekeeper before they can communicate with each other.
13. The gatekeeper finds in its routing tables that this call should be terminated by a termination gateway.
14. The gatekeeper returns to the Main Gateway the IP address of the termination gateway in an ACF message (as part of the RAS signaling).
15. The gateway initiates a call setup to the remote gateway H.323 peer.
16. The termination gateway connects to the destination number through PSTN.
17. The connection between both ends is established.
18. Upon call disconnect, the Main Gateway sends accounting message to the RADIUS with CDR records of the call.

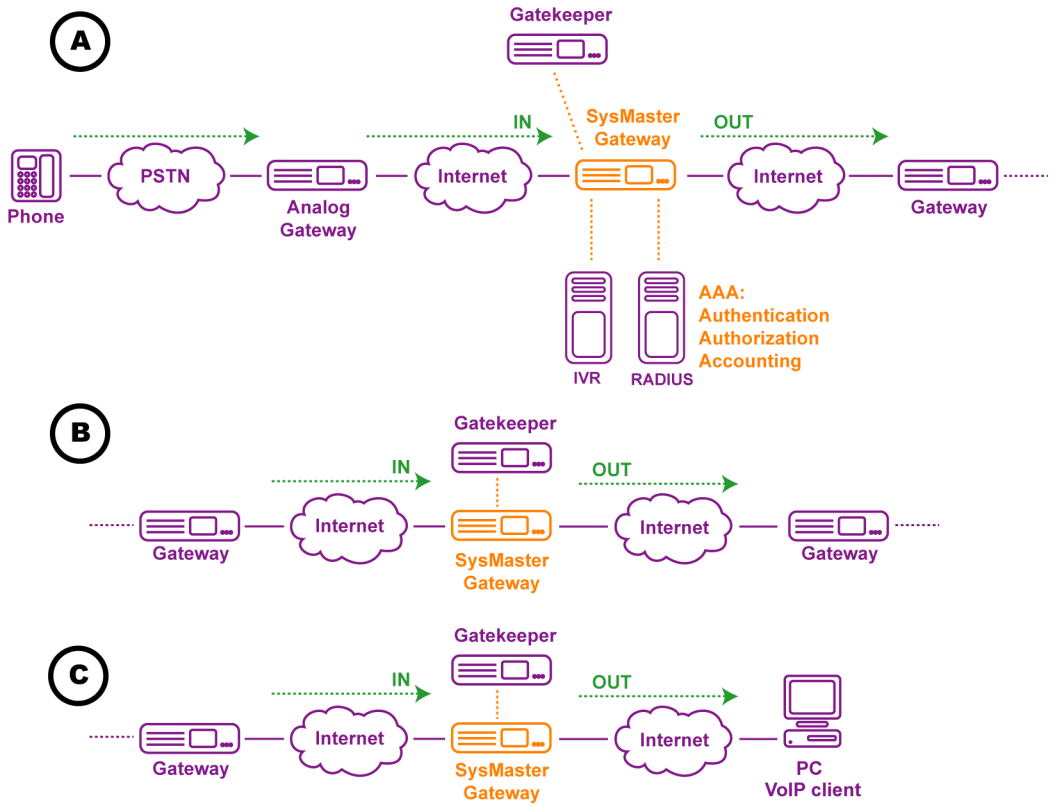
Case B. H.323 Proxy Mode

1. An incoming call request is done.
2. The call filter catches the call based on source number prefixes or by endpoint.
3. The Gateway selects the Incoming Profile as indicated in the call filter.
4. The IVR profile should be Pass-Through indicating no audio services are provided.
5. The RADIUS server selected will be used only for accounting only or AAA purposes (optional).
6. The gateway checks the selected Routing Table and selects the gateway as endpoint to which the outgoing call will be established. It is not allowed to use H.323 Gatekeeper as endpoint. In the case of H.323 proxy, there is no codec translation performed. The

gateway simply redirects all packets of H225, H245, RTP. It can optionally redirect inbound VoIP IVR messages too.

7 After call disconnect, the proxy may send accounting message to the RADIUS server if such one is specified.

VoIP to VoIP



Case C. Termination to VoIP phone or VoIP software PC client

1 An incoming call request is received into the Sysmaster gateway.

2 The call filter catches the call based on source number prefixes or by endpoint.

3 The Gateway selects the Incoming Profile as indicated in the call filter.

4 The IVR profile should be CDR Only indicating no audio services are provided.

5 The RADIUS server selected will be used only for accounting purposes.

6 The gateway checks the selected Routing Table and selects the gatekeeper as an Endpoint

7 SysMaster gateway performs RAS signaling asking for permission to connect to the destination number as well as receive the destination IP address of the destination H.323 peer.

8 The gatekeeper detects that there is an endpoint registered for the destination number.

9 The gatekeeper returns to the SysMaster gateway the IP address of the destination H.323 peer in an ACF message (as part of the RAS signaling).

10 The gateway initiates a call setup to the destination H.323 peer (that can be a VoIP phone or a VoIP software PC client).

11 The connection between both ends is established

12 After call is disconnected, the gateway sends accounting message to the RADIUS with CDR records of the call.

Call Filters

Overview

Call Filters are used on only incoming calls and only before an answer from the call has been received. Call Filters could be viewed as firewalls granting or denying access to remote callers. Incoming calls are authenticated based on ANI or DNIS authentication types, and once the authentication parameters match the call filter, it can accept or reject the incoming call. If incoming calls come from the Internet (e.g. from gateways, gatekeepers, VoIP phones), ANI becomes Source Number, and DNIS becomes Destination Number.

When an incoming call is accepted, the incoming call will be associated with an Inbound Profile for further processing. The inbound call will be processed according to the IVR Profile, Routing Table, RADIUS Server Group, or PBX Group as allocated to it in the Inbound Profile.

Parameters:

Filter Name	Name of the filter.
Priority	Grants a level of priority to the created call filter. The priority can range from 0 to 20. The higher number means higher priority. Priority is used to determine which Call filter will match and process an incoming call when there are two or more matching Call filters. In case more than one Call Filter matches an incoming call, the system tries to resolve which Call filter will take over the call processing by checking the following parameters in the order they appear: ■ Higher priority ■ Longer DNIS ■ Longer ANI
Endpoint	Designated an endpoint to the call filter. The filter rules are applied to the endpoints matching this endpoint. The matching is done based on an IP address.

Mask (0-32)	Specifies the mask of the IP address to be matched. For example mask 24 will enforce matching of the first 3 octets of the IP address of the Endpoint. This way, multiple gateways originating from the same network can match the rules of the filter.
Span	Defines the Span to be matched. The only way to catch PSTN incoming calls is to specify the span they come from. If there are four spans and the system must catch calls from all the spans, there should be a seperate filter for each span. PSTN calls cannot be catched using Dial Groups as an endpoint
ANI Prefix	Specifies that ANI (Automatic Number Identification) Prefix (for calls coming from PSTN) or a Source Number (for calls coming from VoIP channels) prefix that will be used to match incoming calls.
DNIS Prefix	Specifies that DNIS (Dialed Number Identification Service) Prefix (for calls coming from PSTN) or a Destination Number (for calls coming from VoIP channels) prefix that will be used to match incoming calls.
Inbound Profile	Assigns an Inbound profile to the call filter. The Inbound profile is used to further process the call providing IVR, RADIUS, and routing functionality.
Description	Allows a short description (up to 71 characters) of the Call Filter to be entered.
Advanced Rules	Advanced Rules allow for flexible enforcement of the call filter based on time or endpoint availability.

Managing Call Filters

Call Filters should be generally created last following the setting up all other prerequisite resources. The workflow for managing Call Filters is the following:

1. Create the necessary Endpoint, if Endpoint matching will be performed.
2. If Span matching will be performed, make sure all Spans are correctly defined. You can match calls coming from the PSTN lines only through Spans. Should administrators want to match all PSTN traffic, independent of which Span it comes, they should create as many Call Filters as the number of Spans - one Span per Call Filter. All such Call Filter may share the same Inbound Profile processing. Beside this, within a Call Filter administrators can specify even a separate channels, participating in the Call Filter. This provides for finer granularity in differentiating the origin of incoming calls and their subsecuent processing.
3. Prepare the required Inbound Profile to process the matching call. To this end, there should be an appropriate IVR Profile, RADIUS Groups, Routing Table, PBX Group. Some of these may not be required to define an Inbound Profile.

To Add Call Filter

1. From the Navigation tree, select the **Call Processing > Call Filters** node.
2. From the Edit Menu select 'Add Call Filter'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the modifications.
4. In the case, Span filtering is selected - to match calls originating from the PSTN - administrators will have to further edit the definition of the Call Filter. There they will be able to specify which span channels will participate in the call filtering.

To Edit Call Filter

1. From the Navigation tree, select the **Call Processing > Call Filters** node.
2. From the right pane of the Navigator, select the Call Filter to be edited.
3. From the Edit Menu select 'Edit Call Filter'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce the modifications.

To Delete Call Filter

1. From the Navigation tree, select the **Call Processing > Call Filters** node.
2. From the right pane of the Navigator, select the Call Filter to be deleted.
3. From the Edit Menu, select the Delete menu item.

Inbound Processing

Overview

Inbound Profile specifies a set of processing parameters that will be associated with an incoming call. These include the following:

- ANI/DNIS (Sorce/Destination Number) translation
- IVR Profile
- Routing Table
- RADIUS Server Group
- PBX Group

Once an inbound profile for an incoming call has been created, it could be added to the overall call processing by assigning it to a call filter.

DNIS/ANI Translation

DNIS/ANI translation is perofmed in the Inbound processing first. It is necessary so that the supplied numbers are prepared for correct routing. The ANI/DNIS number would be rewritten according to the pattern specified. Each pattern has the form of leftPart = rightPart. The left part is matched against the prefix of the destination number. Each marked text is then replaced with the corresponding text from the right part of the field. The

right part contains list of texts separated with colon (:). If the Left part does not have text marked with [] then the whole left part is marked for replacement.

Examples:

Pattern: '123=456' Number: '123789': new number: '456789'

Pattern: '1[(1:2)]3=456' Number: '123789': new number: '14563789'

Pattern: '1[(1:2)]3S=456' Number: '123789': new number: '14563789'

Pattern: '1[X]3[N]S=456' Number: '123789': new number: '1456389'

Pattern: '@##[123][]X[]=444:55:6' Number: '5555#123789': new number: '5555#444557689'

Pattern: '[]123=444' Number: '123789': new number: '444123789'

Parameters:

DNIS Translation	Defines a DNIS pattern of translations.
ANI Translation	Defines an ANI pattern of translations.
IVR Profile	Assigns and IVR Profile to the inbound profile of the incoming call. System administrators could select an appropriate IVR Profile from the list of available ones.
Routing Table	Associates the inbound profile with a particular already created Routing Table.
RADIUS Group	Specifies the RADIUS Group the inbound profile would belong to.
PBX Group	Specifies the PBX Group the inbound profile would belong to.
Description	Allows a short description (up to 71 characters) of the Inbound Profile profile to be entered.

Managing Inbound Profiles

The workflow for creating Inbound Profile is the following:

1. Plan the appropriate ANI/DNIS number translations. This is necessary for correct routing of the call.
2. Specify an appropriate IVR Profile. In the case, an IVR Profile needs to be created, make sure all Language Servers and language files are in place.
3. Specify an appropriate Routing Table to route the call. If such table does not exist, make create one. For this, you will need to have a provider with provider rates (that serve only for the Least Cost Routing algorithms, and not for billing) as well as Endpoints that will terminate the calls.

4 Specify a RADIUS Group. To this end the system must have configured RADIUS server groups and RADIUS servers in them. You will have to consider what kind of RADIUS services the system will need. i.e. AAA (Authentication, Authorization, Accounting) or Accounting only.

5 Specify a PBX Group. This is necessary if you plan use this Inbound Profile for PBX call processing and routing.

To Add Inbound Profile

1 From the Navigation tree, select the **Call Processing > Inbound Profile** node.

2 From the Edit Menu select 'Add Inbound Profile'.
A dialog box shows up.

3 Fill in the data and click on the Apply button to enforce the modifications.

To Edit Inbound Profile

1 From the Navigation tree, select the **Call Processing > Inbound Profile** node.

2 From the right pane of the Navigator, select the Inbound Profile to be edited.

3 From the Edit Menu select 'Edit Inbound Profile'.
A dialog box shows up.

4 Fill in the data and click on the Apply button to enforce the modifications.

To Delete Inbound Profile

1 From the Navigation tree, select the **Call Processing > Inbound Profile** node.

2 From the right pane of the Navigator, select the Inbound Profile to be deleted.

3 From the Edit Menu, select the Delete menu item.

Outbound Processing

Overview

Outbound Profiles are used by Endpoints before an outgoing call has been established. Creating an Outbound Profile ensures that the endpoint(s) associated with it would be able to translate Caller IDs and Destination Numbers according to the requirements. Endpoints and their respective Outbound Profiles are used in the routing process.

Parameters:

ANI Translation	Defines an ANI pattern of translations. The destination number would be rewritten according to the pattern specified.
DNIS Translation	Defines a DNIS pattern of translations. The destination number would be rewritten according to the pattern specified.

PBX Group	Specifies the PBX Group the outbound profile would belong to.
Description	Allows a short description (up to 71 characters) of the Inbound Profile profile to be entered.

Managing Outbound Profiles

The workflow for creating Outbound Profile is the following:

1. Plan the appropriate ANI/DNIS number translations. They determine how these parameters will send to the call terminating parties.
2. In the case of PBX processing and routing, specify a PBX Profile.

To Add Outbound Profile

1. From the Navigation tree, select the **Call Processing > Outbound Profile** node.
2. From the Edit Menu select 'Add Outbound Profile'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the modifications.

To Edit Inbound Profile

1. From the Navigation tree, select the **Call Processing > Outbound Profile** node.
2. From the right pane of the Navigator, select the Inbound Profile to be edited.
3. From the Edit Menu select 'Edit Outbound Profile'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce the modifications.

To Delete Inbound Profile

1. From the Navigation tree, select the **Call Processing > Outbound Profile** node.
2. From the right pane of the Navigator, select the Inbound Profile to be deleted.
3. From the Edit Menu, select the Delete menu item.

Dial Groups

Overview

Dial Groups represent groups of Endpoints and PSTN Span/channels. Dial Groups creation is in two stages. In the first stage, they are simply created as objects and at the second stage Endpoints are added to them. Each Dial Group has an ID which is used to attach them to an Endpoint. E.g. an Endpoint of type Dial Group can have a local IP address 127.0.0.1:10 where 10 is the ID of the selected Dial Group attached to the endpoint.

Each Dial Group has a Hunt Type determining the way endpoints are accessed in the group. It can be one the following:

- **Sequential/Asc** - the routing result is filled in the order in which the endpoints are defined in the group.
- **Sequential/Desc** - the routing result is filled in the reverse order in which the endpoints are defined in the group.
- **First Available -** Dial Groups of such Hunt Type can have only Span Channels elements (no other endpoints). The gateway selects the first available span channel and attempts a call. If it fails, it doesn't attempt to route the call through another channel.
- **Broadcast** - all endpoints in the group are connected simultaneously. If the number specified in the max result is exceeded, no more connections are tried to be established.
- **Rotation** - acts similarly to the Sequential order but with each call that is terminated in the dial group, the previously top endpoint in the routing result order goes to the bottom of the list.

Parameters:

Dial Group Name	Defines the name of the created dial group. The name could contain any combination of alphabetical and numerical characters.
Hunt Type	Specifies the method according which endpoints would be served by the dial group. Available options are: ■ **Sequential/Asc** Routing result is always obtained from the first endpoints in the dial group. ■ **Sequential/Desc** Routing result is always obtained by the last endpoints in the dial group ■ **First Available** ■ **Broadcast** All endpoints in the dial group are present in the routing result. The amount of endpoints present could be controlled by the value of the "Max Results" field. ■ **Rotation** Endpoints are chosen in a manner identical to Sequential/Asc. The difference being that every other routing result will be obtained by the next endpoint in the dial group.
Max Results (1-500)	Defines how many endpoints of a dial group could be present in the routing result. The routing result is an ordered list of Endpoints to which the gateway attempts to route a call.

Connect Timeout (1-120)	Denotes the period of time (in seconds) beyond which dial group connection attempts will be terminated. The dial group connect timeout period could be in the range of 1 to 120 seconds
ACQ Profile	Specifies the ACQ Profile assigned to the dial group.

Managing Dial Groups

The workflow for creating Dial Groups is the following:

1. Plan the appropriate Hunt Type. If you plan to use the gateway to terminate to PSTN, then the Rotating algorithm is most suitable.
2. Select a proper Max Results number. You may want to select smaller number up to the number of call lines. Max Result is responsible for the length of the list of possible lines/ endpoints ready to be used to put the call through.
3. Select an Appropriate ACD Profile. ACD (Automatic Call Distribution) Profiles are suitable for PBX call processing.
4. Plan the Endpoints, Spans and Channels to be used in this Dial Group. Nesting of Dial Groups is not allowed.

To Add Dial Group

1. From the Navigation tree, select the **Call Processing > Dial Group** node.
2. From the Edit Menu select 'Add Dial Group'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the modifications.
4. To specify the spans and channels assigned to a Dial Group proceed with Editing the Dial Group once it is created.

To Edit Dial Group

1. From the Navigation tree, select the **Call Processing > Dial Group** node.
2. From the right pane of the Navigator, select the Dial Group to be edited.
3. From the Edit Menu select 'Edit Dial Group'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce the modifications.

To Delete Dial Group

1. From the Navigation tree, select the **Call Processing > Dial Group** node.
2. From the right pane of the Navigator, select the Dial Group to be deleted.
3. From the Edit Menu, select the Delete menu item.

ACD (Automatic Call Distribution)

Overview

ACD is a module allowing administrators to define various behaviors(profiles) for call distribution within a dial group. Each Dial Group can be bound to only one ACD profile. Attaching small number of manageable ACD profiles to a large number of Dial Groups, allows for easy readjustment of the ACD rules for multiple Dial Groups at a time.

Parameters:

Name	Defines the name of an ACD profile.
Music On Hold	Specifies the name of the music-on-hold file to be played while calls are in queue.
Calls to Start Queueing	Specifies the number of concurrent calls to a dial group after which the gateway will put calls in queue. Generally, this number should be the number of endpoints within a dial group to which the ACD profile is attached.
Calls to Refuse Queueing	Specifies the number of concurrent calls to a dial group after which the gateway will drop incoming calls.
Greeting Iverval (sec)	Indicates the time interval at which greeting message is played.
Auto Retry Call Interval (sec)	Specifies the interval at which queued calls attempt to connect.

Managing ACD Profiles

To Add ACD Profile

1. From the Navigation tree, select the **ACD > ACD Profiles** node.
2. From the Edit Menu select 'Add ACD Profile'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the modifications.
4. To specify the spans and channels assigned to a ACD Profile proceed with editing the selected ACD Profile once it is created.

To Edit ACD Profile

1. From the Navigation tree, select the **ACD > ACD Profiles** node.
2. From the right pane of the Navigator, select the ACD Profile to be edited.
3. From the Edit Menu select 'Edit ACD Profile'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce the modifications.

To Delete ACD Profile

1. From the Navigation tree, select the **ACD > ACD Profiles** node.
2. From the right pane of the Navigator, select the ACD Profile to be deleted.
3. From the Edit Menu, select the Delete menu item.

Music On Hold

Overview

The Music On Hold module controls the music played to callers while waiting in queue. The module allows administrators to create multiple Music-on-hold profiles for modular assignment to ACD profiles. Each Music-on-hold profile contains multiple files that are played to the waiting callers.

Music-On-Hold Profiles

Music-on-hold profiles can only be created and deleted. Modifying is not possible.

Parameters:

Name	Defines the name of an Music-On-Hold profile. The profile is listed in the tree for adding Musc-on-hold files.

Managing Music-On-Hold Profiles

To Add Music-on-hold Profile

1. From the Navigation tree, select the **Music On Hold > Music-On-Hold Profiles** node.
2. From the Edit Menu select 'Add Profile'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to complete the creation.

To Delete Music-on-hold Profile

1. From the Navigation tree, select the **Music On Hold > Music-On-Hold Profiles** node.
2. From the right pane of the Navigator, select the Delete Profile to be deleted.
3. From the Edit Menu, select the Delete menu item.

Music-On-Hold Files

Music-on-hold files are the actual music files that are played. The accepted audio format is **wave, au, gsm.** where PCM - uLaw 8kHz - is for ".au" extension and GSM for ".gsm" extension.

Parameters:

New File Name	Defines the name of an Music-On-Hold file.

Managing Music-On-Hold Files

To Add Music-on-hold File

1. From the Navigation tree, select the **Music On Hold > Music-On-Hold Files** node.
2. From the Edit Menu select 'Upload File'.
   A dialog box shows up.
3. Click on the "Browse" button and locate the file to be uploaded.
4. Click on the Process File to actully upload the file.

To Rename Music-on-hold File

1. From the Navigation tree, select the **Music On Hold > Music-On-Hold Files** node.
2. From the right pane of the Navigator, select the file to be renamed.
3. From the Edit Menu, select the Rename File menu item.

To Delete Music-on-hold File

1. From the Navigation tree, select the **Music On Hold > Music-On-Hold Files** node.
2. From the right pane of the Navigator, select the Delete File to be deleted.
3. From the Edit Menu, select the Delete menu item.

Chapter 4 Provider Setup

Overview

A provider is a telco company that provides its VoIP equipment and infrastructure to the Management company to terminate VoIP calls made through the gateways/gatekeepers of the Management company. The provider company can provide either gateways or gatekeepers to terminate calls. The SysMaster digital gateway uses provider definitions to:

1. Implement route failover.
2. Implement least cost routing of calls based on an algorithm for selecting the least expensive route.
3. Collect CDR records for calls through all providers.

To accomplish the tasks listed above, the system introduces the following objects:

- **Provider** - a telco company providing VoIP termination services;
- **Provider rate** - a rate definition assigned to a area code location.

In order for the system to use the provider rates data, the system allows you to attach a provider an endpoint as well as attach provider to a route. This way the system can access information about providers and their rates and take call routing decisions based on the routing rules. For more information please refer to the routing section.

Provider

Parameters:

Provider Name	Designated the name of the provider. The name could contain any combination of numerical and alphabetical characters.

Provider Rates

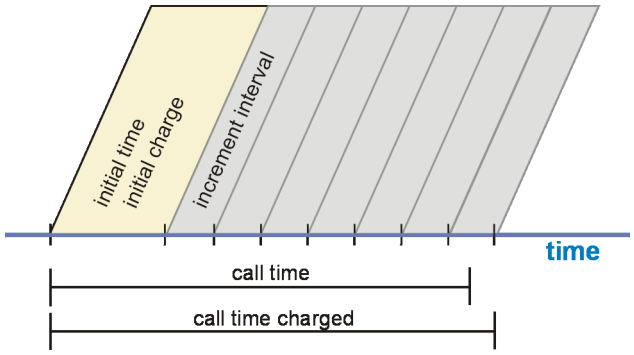
Parameters:

Provider	Designated the name of the provider.

Location	Denotes the name of the location the newly created rate would apply to. In most instances, a location is referred as the geographical area encompassing a single or a number of area codes.
Area Code	Assigns the unique area code the newly created rate would apply to. The area code should correspondent to the location entered above.
Init Time (sec)	Specifies the duration (in seconds) of the initial time period. The initial time period (interval) starts from the moment when a call is placed and ends based on the value entered in the Init Time field.
Init Charge (cents)	Allocates the amount (in US cents) that would be charged during the initial time period (Init Time) of the call.
Sample Time (sec)	Specifies the duration of the Sample Time (interval) period. The Sample Time period represents at what duration the call would be billed. If a call is to be billed on per minute bases, the Sample Interval must be 60 sec. If no Sample Time is entered, the system will assign a default Sample Time value of 0.
Sample Charge (cents)	Specifies the amount (in US cents) that would be charged on per Sample Time basis. **NOTE:** Sample Charge charges are not charges per second, but charges per Sample Time. To calculate per second call charges Sample Rate should be divided by Sample Interval. **Sample Charge / Sample Time = per second charges**
Increment Time (sec)	Specifies the value of the time increment to be applied to the base duration of the call. The Increment Time value would represent a single time unit that would be used in segmenting the call for billing purposes. **For instance:** If the Increment Time is specified as 10 sec and a user initiates a call for 31 sec, the call would be segmented into 4 billing time units. As a result the user would NOT be charged for the 31 sec of call time but for 40 sec call time.
Call Origination Charge (cents)	Specifies the amount (in US cents) imposed on the management company by the Call Origination Provider. Call Origination Provider is network provider offering services at the point of call origination. Call origination charges represent an expense to the management company.

Call Termination Charge (cents)	Specifies the amount (in US cents) imposed on the management company by the Call Termination Provider. Call Termination Provider is network provider offering services at the point of call termination. Call termination charges represent an expense to the management company.

The figure below visually explains the meaning of the rate attributes.



Provider Setup

Provider Management

To Add a Provider

1. From the Navigation tree, select the **Provider Management > Provider** node.
2. From the Edit Menu select 'Add Provider'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the provider creation. During provider creation, the system assigns an unique ID of the provider for further reference.

To Edit a Provider

NOTE: Changes made to currently existing provider definitions will propagate throughout the entire system i.e. endpoint, provider rate, area code route definitions.

1. From the Navigation tree, select the **Provider Management > Provider** node.
2. Select the node to be edited and from the Edit Menu select 'Edit Provider'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the changes.

To Delete a Provider

NOTE: Deleting a provider will automatically delete a all relating provider rates, endpoints defined for the provider, as well as area code routes for the provider.

1. From the Navigation tree, select the **Provider Management > Provider** node.
2. Select the node to be deleted and from the Edit Menu select 'Delete Provider'.
3. The delete command will be completed and the list with providers refreshed.

Provider Rate Management

Provider rates are defined per provider. The system will logically allow you to create provider rates only for existing providers. As mentioned earlier, provider rates do not participate in call billing but only to hint the system how to intelligently route calls based on least call routing. Rates are defined per area code. The area code may be simply the first number of an area code, not necessary the full area code to a destination.

You can add provider rates in two ways: either through the add dialog, or from the Import command.

To Add a Provider Rate through the Add Rate Dialog

1. From the Navigation tree, select the **Provider Management > Provider Rates > [a specific provider]** node.
2. From the Edit Menu select 'Add Provider Rate'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the provider rate creation.
   Please, pay special attention to the area code data you fill in.

In order to use the Import dialog, to import rates you have to comply with the following comma separated data format:

```
"Country", "Area Code", "Init Time", "Init Charge", "Sample Time",
"Sample Charge", "Increment Time", "Call Origination Charge", "Call
Termination Charge"
```

Example:

```
usa, 1, 10, 60, 1, 10, 0, 2, 2

can, 2, 10, 60, 1, 10, 0, 2, 2
```

To Add Provider Rates through the Import Dialog

1. From the Navigation tree, select the **Provider Management > Provider Rates > [a specific provider]** node.
2. From the Edit Menu select 'Import Provider Rate'.
   A dialog box shows up.
3. Specify the local file and click on the Apply button to import the rates.

TIP: The Provider Rates node in the tree lists all providers as tree nodes. There is a bracketed number indicating system ID of the respective provider.

To Edit a Provider Rate

1. From the Navigation tree, select the **Provider Management > Provider Rates > [a specific provider]** node.
2. From the list of rates in the right pane, select the rate to edit. From the Edit Menu select 'Edit Provider Rate'. A dialog box shows up.
3. Edit the settings to be changed and click on the Apply button to enforce the changes.

TIP: The provider rates list in the right pane of the Navigation window has a tab named 'Is Modified' that indicates whether a rate has been modified once it has been created (either through the Add dialog or through Rates import operation).

To Delete a Provider Rate

1. From the Navigation tree, select the **Provider Management > Provider Rates > [a specific provider]** node.
2. From the list of rates in the right pane, select the rate to edit. From the Edit Menu select 'Delete Provider Rate'.
3. The delete command will be completed and the list with provider rates will be refreshed.

To Delete All Provider Rates

1. From the Navigation tree, select the **Provider Management > Provider Rates > [a specific provider]** node.
2. From the Edit Menu, select 'Delete All Provider Rates'.
3. The delete command will be completed and the list with provider rates will be emptied.

To Export All Provider Rates of a Provider

1. From the Navigation tree, select the **Provider Management > Provider Rates > [a specific provider]** node.
2. From the Edit Menu select 'Export Provider Rates'.
3. A popup window will prompt you to download a text file containing all provider rates in a comma separated format. The format is the same as the one used to import rates.

Provider Call History

The SysMaster gateway allows the administrators to view detailed call records for calls that have been terminated by the respective provider. Furthermore, administrators can export CDRs for billing purposes or additional further data processing.

To Export All CDRs for a Provider

1. From the Navigation tree, select the **Provider Management > Provider Call History > [a specific provider]** node.

2 From the tree, select a provider node to view its calling history in the right pane of the Navigator.

3 From the Menu, select the 'Export Call History' menu. A popup window will prompt you to save the data to your local computer. The data is exported in comma-separated text format.

The SysMaster gateway interface provides a convenient tool to interactively view call history using relevant time and area code filters.

To View Call History

1 From the Navigation tree, select the **Provider Management > Provider** node.

2 A list of all providers will appear in the right pane of the navigator. Select the provider for which call history data will be viewed.

3 From the Menu, select the 'Call History' menu. A new window will show up. In this window, you can view monthly and daily call history records for calls that have been terminated by the respective provider.

To View Call History by Time

1 Click on the month/day link to drill down to CDR data for the month/day selected.

2 At each stage of drilling down you will see aggregated data for the selected period (month or day)

3 Use the navigational helpers to navigate to the desired level of time. These links are located at the top of the table.

To View Call History Filtered By Area Code

1 The Navigate to the desired level for which the filter will work (e.g. specific day, month etc.)

2 Hit the search button to show all calls that match the filter criteria.

The Call Detail Records have the following parameters:

Calls/Successful	Specifies the successful to failed call ratio. This is for all calls that has been routed through the selected provider.
Average Latency(sec)	The average latency for the duration of the call.
Average Successful Rate (ASR)(%)	Specifies the successful to failed calls ratio.
Originated	Specifies the number of call that have been originated from the provider.
Answered	Specifies the number of calls that have been terminated (answered) by the provider.

Average Cost	Specifies the average cost for the calls that have been routed through the selected provider. The price is calculated based on the provider rates for the respective provider.
Call Time	Calling time for the duration of the routed calls.
Incoming Bytes	Specifies the inbound VoIP data volume in bytes with respect to the SysMaster gateway for the duration of the calls.
Outgoing Bytes	Specifies the outbound VoIP data volume in bytes with respect to the SysMaster gateway for the duration of the calls.
Incoming Packets	Specifies the inbound VoIP data volume in IP packets with respect to the SysMaster gateway for the duration of the calls.
Outgoing Packets	Specifies the outbound VoIP data volume in IP packets with respect to the SysMaster gateway for the duration of the calls.

Chapter 5 PSTN Setup

Span Configuration

OverviewRADIUS

Spans represent trunks (spans) of T1/E1/ISDN digital PSTN lines. The SysMaster gateway supports T1/E1/ISDN lines according to the installed voice card.

T1 Spans usually support 23+1 channels, i.e. 24 channels in CAS mode and 23+1 channels in ISDN mode (one D channel). The channel allocation is as follows: CAS uses 24 voice channels; ISDN uses 23 voice channels (channel 24 is used for D channel).

E1 Spans support 31 channels in CAS mode and 30 B channels and one D channel in ISDN mode. The channel allocation is as follows: CAS uses 30 voice channels (1-15,17-31 for voice and 16 for signaling).

ISDN uses 30 voice channels (channel 16 is used for D channel).

Spans can be used in:

- Call Filters to filter incoming calls from the PSTN lines
- Dial Groups, and this way they can participate indirectly in Endpoints. Endpoints can be used in Routing tables for outgoing call routing. This is why, attaching spans and channels to Dial Groups is the only way to route calls to the PSTN side.

The SysMaster gateway automatically detects the settings of the T1/E1 PSTN card that is installed on the device.

Parameters:

Span ID	Specifies the sequence number (ID) of the PSTN span. Supported numbers are: Span ID: #1 Span ID: #2 Span ID: #3 Span ID: #4

Span Status: Enabled / Disabled	If enabled, the channels within the span can be used, otherwise they will be blocked.
Signalling	Specifies the signaling type of the digital voice line. CAS (Channel Associate Signaling): used for channeling the service. Each channel represents a phone line. The signaling data is sent on the same data channel. ISDN PRI there are two options for signaling: ■ CPE (Customer Premises Equipment) ■ Network Side
Span Name	Assigns a name to the created Span.

Span Management

To Add Span Configuration

1. From the Navigation tree, select the **PSTN/TDM Management > Span Configuration** node.
2. From the Edit Menu select 'Add Span Configuration'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the modifications.

To Edit Span Configuration

1. From the Navigation tree, select the **PSTN/TDM Management > Span Configuration** node.
2. From the right pane of the Navigator, select the Span Configuration to be edited.
3. From the Edit Menu select 'Edit Span Configuration'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce the modifications.

To Delete Span Configuration

1. From the Navigation tree, select the **PSTN/TDM Management > Span Configuration** node.
2. From the right pane of the Navigator, select the Span Configuration to be deleted.
3. From the Edit Menu, select the Delete menu item.

Channel Configuration

Overview

A Channel represents a bandwidth allocation within a Span enough to accomodate one call leg. A single call between two parties requires one channel for each party.

There are two kinds of channel signaling:

- Loop Start and Ground Start use Dial Tones for start, and only DTMF signaling (Dual Tone Multi-Frequency).
- E & M (Ear and Mouth) use Immediate or Wink methods for start, and MF (Multi-Frequency), or DTMF (Dual Tone Multi-Frequency) signaling.

Loop Start and Ground Start do not provide DNIS (Dialed Number Identification Service, called party number) and ANI (Automatic Number identification, the calling party number) address information. Such address information can be sent from the telephone company by using other methods such as E&M.

Loop Start is the most used signaling for analog and digital lines. On T1 lines the signaling uses bits A and B. The method is susceptible to glare and should not be used on bi-directional lines where both ends can place calls simultaneously.

Ground Start is similar to Loop Start but provides immediate seizure indication to avoid the glare.

The Loop Start and Ground Start signaling can be provided to different parties:

- Foreign Exchange Office (FXO) signaling: this signaling is provided to FXS devices (inside phones or PBXs systems).
- Foreign Exchange Station (FXS) signaling: this signaling is provided to CO lines or outside PBXs.

There are other methods that provide two-way calling, all based on E&M:

- E&M Wink Start: the caller waits for wink (the called party should go off-hook for short period of time). Then the caller sends the address information.
- E&M Immediate: the caller does not wait for wink before sending address information.

There are extensions to the E&M signaling:

- E&M Feature Group B (MF): this method uses Multi-Frequency and can provide DNIS address information.
- E&M Feature Group D (MF): this method uses Multi-Frequency and can provide ANI and DNIS address information.
- E&M Feature Group D (DTMF): this method uses Dual Tone Multi-Frequency and can provide ANI and DNIS address information.

Parameters:

Channes: Available / Assigned	Specifies the available channels to be assigned to the channel configuration setting.
Signal Type	Allows a signal type to be selected. Used when span signaling is set to CAS.

Tx Gain (-20dB:20dB)	Specifies the value for the Tx Gain. The Tx Gain is used to amplify the transmitted voice level. The Tx Gain could only be adjusted in the range of -20.0 - +20.0 db.
Rx Gain (-20dB:20dB)	Specifies the value for the Rx Gain. The Rx Gain is used to amplify the received voice level. The Rx Gain could only be adjusted in the range of -20.0 - +20.0 db.
Accept Caller ID	Specifies whether the Caller ID for an incoming call to be accepted or not.
Caller ID	Specifies Caller ID to use for incoming calls. It is used only for FXO signaling. If the number of the Caller ID ends with '+' sign, it will be replaced with a channel number. For example: - Assigned Caller ID: 1234, Resulting Caller ID: 1234 - Assigned Caller ID: 1234+, Resulting Caller ID for channel 24: 123424
Time Rule	

Channel Management

To Add Channel Configuration

1. From the Navigation tree, select the **PSTN/TDM Management > Channel Configuration > [Span]** node. All nodes under channel configurations represent the spans that are active.
2. From the Edit Menu select 'Add Channel Configuration'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the modifications.

To Edit Channel Configuration

1. From the Navigation tree, select the **PSTN/TDM Management > Channel Configuration > [Span]** node.
2. From the right pane of the Navigator, select the Span Configuration to be edited.
3. From the Edit Menu select 'Edit Channel Configuration'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce the modifications.

To Delete Channel Configuration

1. From the Navigation tree, select the **PSTN/TDM Management > Channel Configuration > [Span]** node.
2. From the right pane of the Navigator, select the Channel Configuration to be deleted.
3. From the Edit Menu, select the Delete menu item.

Chapter 6 Call Routing

Endpoints

Overview

An endpoint is associated with the party to which a call setup could be made or with the party from which calls could be received by the Management Company. In accordance to the direction of the call flow an endpoint could be either Incoming (a call has been placed towards us) or Outgoing (a call has been placed from us).

Each endpoint created refers to a designated Provider. When output routing is performed the desired endpoint is determined on the basis of its associated Provider.

NOTE: Endpoints of type H.323 should be assigned a status of **active/local listener** when created.

Types of endpoints

H.323 Gateway

H.323 Gateway is an entity that communicates using the H.323 set of protocols. It translates PSTN packets into IP packets and vice versa. The former is called encoding and the latter - decoding. H323 Gateways are used by H.323 gateway or by H.323 Proxy for incoming or outgoing calls. If a gatekeeper is specified as a controller/gatekeeper, then the gateway uses the gatekeeper to send ARQ (Admission Request) message over the RAS channel to it. The gateway waits for Request Confirm or Request Reject messages.

H.323 Gatekeeper

H.323 Gatekeepers can be used as outgoing endpoints as well as RAS (Registration, Admission and Status) channel for incoming and outgoing calls of the H.323 gateway.

If a Gatekeeper is specified then the gateway can receive calls from its IP, without performing RAS signaling for it.

When a Gatekeeper is used as an endpoint, it can redirect a call to a remote H.323 endpoint but the system needs to know only about the gatekeeper itself. In addition, the gatekeeper can perform number translation, bandwidth control as well as other tasks related to call processing.

When a Gatekeeper is specified as a controller for H.323 gateway, all incoming and outgoing calls, the gateway use RAS signalling through it. In this way the Gateway binds itself to the Gatekeeper.

H.323 Proxy

H.323 is a special mode of work of the H.323 gateway where it simply redirects VoIP messages. It does not change the encoding of the messages. It can use RADIUS processing optionally as well as use a special type of IVR (pass-through) instructions. Authentication is done via tech-prefixes. This mode can be used as a tool to hide the source of your voice traffic.

By default, H.323 Gateway listens at all IP addresses at port 1720 or at specified Gateway Listen IP addresses. If a gateway uses both as a H.323 gateway and H.323 proxy, there could be port contention because H.323 uses port 1720 too. This is why H.323 Proxy and H.323 Gateway should not have common Listen IP addresses.

On the other hand it is recommended that Listen IP addresses are specified in order to escape common resource interference. When using the gateway as both H.323 Gateway and H.323 Proxy, the system check procedures stop services with no specific Listen IP address assigned (as the lack of a specific Listen IP address indicates the gateway will listen at all available IP addresses).

Callback Server

The Callback server endpoint denotes the callback functionality of the SysMaster gateway. It can work in several modes based on the authentication mode as well as the way it is requested - web request, email, SMS message or the way authentication is done - ANI, PIN, DID.

SIP Gateways

SIP Gateways are similar to H.323 Gateways with the main difference that they can specify a Default Source number to be used in outgoing calls. This IP address should be present in the list of IP addresses of the SIP gateway or to be a Local IP address in the cases when the Listen IP address is 0.0.0.0 (i.e. all IP addresses).

SIP Registrars

SIP Registrars are used for registration of the SIP Gateway ID together with its IP address in a registry. This way the gateway is known to other SIP Peers through its registered name. All such registration is being refreshed on a timely bases which is useful if the SIP Gateway host changes its IP address.

Dial Group

Dial Groups represent aggregated entity of other endpoints or PSTN spans/channels. A Dial Group cannot contain other dial groups.

Call Drop Endpoint

This type of endpoint is used to drop calls. It can be used in building blocking call filters for dropping calls with certain parameters such as ANI, DNIS, SPAN, ENDPOINT.

Parameters:

Name	Name of the endpoint. The name could consist of any combination of alphabetical or numeric characters.
IP	Specifies the IP address of the endpoint.
Type	Specifies what type of the endpoint.
Status	Indicates whether the endpoint is active or disabled. An endpoint could also be related to a local or remote IP address by selecting the active/local listener status.
GK/SIP Controller	Assigning a GK/SIP Controller to an endpoint ensures that the endpoint would be able to facilitate RAS messaging.
Number of Ports (1-1000)	Defines the number of ports available to the endpoint. The number of ports represents the maximum number of calls allowed to the endpoint.
Priority (0-20)	Assigns a level of priority to the endpoint. The higher the number the higher priority would be assigned to the endpoint. A higher level of priority of an endpoint means that the endpoint will have a better chance participating in the route of the outgoing call.
Description	Allows a short description (up to 71 characters) of the endpoint to be entered.
Provider Name	Designates the name of the provider the endpoint will be associated with.
Outbound Profile	Specifies the outbound profile the endpoint will be associated with.
Country	Specifies the country where the endpoint is located.
Min Digits (0-10)	Specifies the minimum destination number digits in order for the system to put a call through this endpoint.
Available Codecs	Specifies the codecs that are supported. Administrators can chose only from the listed set of codecs. The assigned codecs should be listed in order of their preference.
Jitter (20-10000 msec)	Specifies the Jitter Buffer selection. Jitter is used to buffer incoming packets to allow for high latency networks to support VoIP communication. The recommended settings are between 50 and 300 ms jitter buffer.

Timeout (1-120)	For Gatekeepers only. Specifies the timeout between retransmissions of the RAS (Registration, Admission and Status - H.225.0) messages.
Default Source IP	Specifies the source IP address for the endpoint. Used only for SIP gateways.
Fast Start	If selected, Fast Start VoIP negotiation would be enabled and a faster call setup would be performed. Make sure the endpoint needs to support this feature.
H.245 Tunneling	The feature allows H.245 messages the use the existing H.225 Transmission Control Protocol (TCP). Make sure the endpoint needs to support this feature.
Silence Suppression	Designates that the endpoint supports Silence Suppression capable VoIP voice processing. Make sure the endpoint needs to support this feature.

Endpoints Management

To Add Endpoint

1. From the Navigation tree, select the **Route Management > Endpoint Configuration** node.
2. From the Edit Menu select 'Add Endpoint'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the modifications.

To Edit Endpoint

1. From the Navigation tree, select the **Route Management > Endpoint Configuration** node.
2. From the right pane of the Navigator, select the Endpoint to be edited.
3. From the Edit Menu select 'Edit Endpoint'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce the modifications.

To Delete Endpoint

1. From the Navigation tree, select the **Route Management > Endpoint Configuration** node.
2. From the right pane of the Navigator, select the Endpoint to be deleted.
3. From the Edit Menu, select the Delete menu item.

Route Tables and Routes

Overview

Routing Tables are used to determine to what Endpoints an incoming call can proceed as an outgoing call. Routing tables represent a lit of pairs of a phone number prefix against an endpoint thus indicating a route. Routing tables are assigned from an Inbound profile and in its turn, an Inbound profile is selected from a call filter.

The VoIP routing searches for the destination number only in the selected by the Inbound profile Routing table.

When the gateway performs call routing it internally builds a list of endpoints through which the call will be routed. The top endpoint of the list is attempted first. If it fails, the next one is attempted, and so on until the call is finally routed. The gateway takes into account the following factors when building its internal routing list for a call:

- If an endpoint has bigger number for priority, then it is preferred;
- Next in the list come the endpoints with lesser cost. The cost is taken from the provider rates for the provider assigned to the Endpoint.

The result represent Endpoints and Dial Groups (wrapped in Endpoints) through which the call should be redirected.

For each Endpoint from this list an Outbound Profile is used according to the one attached in the respective Endpoint definition.

Routing Table Definition Parameters:

Routing Table	Name of the routing table.
Enable Auto Failover	Autofailover allows the routes to use numerous endpoints for termination provided such endpoints are available for the same route.
Timeout (1-300 sec)	Denotes the period of time (in seconds) beyond which routing query will be terminated. The routing timeout period could range from 1 to 300 seconds.

The format of the routing tables is as follows:

"Area Code", "Endpoint IP", "Provider ID", "Cost", "Preferred"

Routes Management

The workflow for managing routes is the following:

1. Create a provider.
2. Define Endpoints that should belong only to one provider.

3 Add Area code rates. The area codes may be simply prefixes (e.g. 3, 5, 22, 454 etc.). Adding rates for Area Code prefixes determines available prefixes a provider covers

4 Create Routing (Routing Table) by assigning which area codes will be in the table

To Add Route Table Definition (Route)

1 From the Navigation tree, select the **Route Management > Routes** node.

2 From the Edit Menu select 'Add Route'.
A dialog box shows up.

3 Fill in the data and click on the Apply button to enforce the modifications.

To Edit Route Table Definition (Route)

1 From the Navigation tree, select the **Route Management > Routes** node.

2 From the right pane of the Navigator, select the Route to be edited.

3 From the Edit Menu select 'Edit Route'.
A dialog box shows up.

4 Fill in the data and click on the Apply button to enforce the modifications.

To Delete Route Table Definition (Route)

1 From the Navigation tree, select the **Route Management > Route** node.

2 From the right pane of the Navigator, select the Route to be deleted.

3 From the Edit Menu, select the Delete menu item.

To Import Route Tables

1 From the Navigation tree, select the **Route Management > Route Table > [Route Table]** node.

2 From the tree, select the Route Table to import data into.

3 From the Edit Menu select 'Import Routes'.
A dialog box shows up.

4 Hit on the Browse button to locate the file to import from. The files should be in the following comma delimited format:
"Area Code", "Endpoint IP", "Provider ID", "Cost", "Preferred"

5 When ready, Click on the Import button to complete the procedure.

To Export Route Tables

1 From the Navigation tree, select the **Route Management > Route Table > [Route Table]** node.

2 From the tree, select the Route Table from which data will be exported.

3 From the Edit Menu, select the Export menu item.

4 A dialog will prompt you to save the file. CLick on the Save button to save the file.

To Delete a Single Route or All Routes

1. From the Navigation tree, select the **Route Management > Route Table > [Route Table]** node.
2. From the right pane of the Navigator, select the Route Table entry to be deleted (for single deletion).
3. From the Edit Menu select 'Delete Route' - for single deletion, or 'Delete All Routes' for deleting all entries.

Chapter 7 RADIUS Server Setup

Overview

SysMaster Gateway needs a RADIUS (Remote Authentication Dial In User Services) server to authenticate and authorize call parties and at the end of to send CDR data for accounting (billing) purposes. The RADIUS server adds a layer of security on the layer of voice communication service provided. The SysMaster Gateway complies with the RADIUS protocol and can communicate with any server conforming to the standards.

For the purposes of authentication and authorization, the SysMaster Gateway can work with only one RADIUS server per call. On the other hand, for the purposes of accounting the gateway can contact multiple RADIUS servers simultaneously.

The gateway represents a NAS (Network Access Server) client to the RADIUS server. The NAS communicates with the RADIUS server through a password - called shared secret.

The administrators of the system should attach a RADIUS server group to each Inbound Profile. The Inbound Profile is used to assign to prefiltered incoming calls a RADIUS Group, IVR Profile, Routing Table, PBX group (if a PBX is installed).

RADIUS Server Groups

Introduction

The SysMaster Gateway can communicate with multiple RADIUS servers simultaneously. In order to separate RADIUS servers for each defined provider, the system uses RADIUS Server Groups to group RADIUS servers responsible for a provider. Within a group there can be multiple RADIUS servers all of which can handle accounting requests simultaneously. Within a server group there can be only one server handling authentication requests together with authorization.

Parameters:

Name	Specifies the name of the server group.
Timeout (1-60 sec)	Defines the period of time (in seconds) for timeout of the server query. RADIUS Server Group timeout could range from 1 to 60 seconds.

Retry Count (1-10)	Defines the number of times one query will be submitted to the RADIUS server. Once the number of retries is over then the system will fail-back to the next RADIUS server in the RADIUS Group.
NAS IP Address	Specifies the IP address of the Network Access Server (which is the SysMaster gateway) from which it will communicate with the RADIUS server. The system allows you to select from the IP addresses that are defined for the gateway. The gateway and the RADIUS server preferably should reside in the same network.
Description	Allows a short description (up to 71 characters) of the conference profile to be entered.

RADIUS Server Group Management

To Add a RADIUS Server Group

1. From the Navigation tree, select the **RADIUS Management > RADIUS Server Group** node.
2. From the Edit Menu select 'Add RADIUS Server Group'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the Server Group creation.

To Edit a RADIUS Server Group

1. From the Navigation tree, select the **RADIUS Management > RADIUS Server Group** node.
2. From the right pane of the Navigator, select the Server Group to be edited.
3. From the Edit Menu select 'Edit RADIUS Server Group'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce the Server Group modification.

To Delete a RADIUS Server Group

1. From the Navigation tree, select the **RADIUS Management > RADIUS Server Group** node.
2. From the right pane of the Navigator, select the Server Group to be deleted.
3. From the Edit Menu select 'Delete RADIUS Server Group'.

RADIUS Servers

Introduction

RADIUS servers are defined with the gateway so that the gateway knows how where to authenticate, authorize and send accounting information for the calls that go through it. RADIUS servers are defined within server groups. Within a Server Group, only one

RADIUS server can be responsible for authentication/authorization while all other RADIUS servers defined within the group should be for accounting only.

Parameters:

Name	Specifies the name of the RADIUS server.
Type	Specifies the type of the RADIUS server. Available options are: ■ ***Disabled*** This option disables the server within the server group it is defined. ■ ***AAA*** This option specifies the server will be used for authentication, authorization and accounting. ■ ***Accounting*** A RADIUS server of this type, should be used only for accounting. The gateway uses it to send CDR records at the end of every call. Before the CDR records are sent, a login authentication request is sent. ■ ***Accounting RFC*** This option indicates that the server will perform similar task as a server of type Accounting. The difference is that there is no login authentication procedure before the gateway sends the CDR records.
IP Address	Specifies the IP Address of the RADIUS server.
Shared Secret	Specifies password through which the gateway device will authenticate itself and initiate a communication session with the RADIUS server.
Port	Specifies the port at which the RADIUS server listens at. Usually the port number is 1812/1813.

RADIUS Server Management

To Add a RADIUS Server

1. From the Navigation tree, select the **RADIUS Management > RADIUS Servers > [RADIUS Server]** node.
2. From the Edit Menu select 'Add RADIUS Server'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the RADIUS Server creation.

To Edit a RADIUS Server

1. From the Navigation tree, select the **RADIUS Management > RADIUS Servers > [RADIUS Server]** node.
2. From the right pane of the Navigator, select the RADIUS Server to be edited.
3. From the Edit Menu select 'Edit RADIUS Server'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce the RADIUS Server modification.

To Delete a RADIUS Server

1. From the Navigation tree, select the **RADIUS Management > RADIUS Servers > [RADIUS Server]** node.
2. From the right pane of the Navigator, select the RADIUS Server to be deleted.
3. From the Edit Menu select 'Delete RADIUS Server'.

To Delete a All RADIUS Servers

1. From the Navigation tree, select the **RADIUS Management > RADIUS Servers > [RADIUS Server]** node.
2. From the Edit Menu select 'Delete All RADIUS Servers'.

Chapter 8 IVR Setup

Introduction

The SysMaster Gateway features a flexible IVR (Interactive Voice Response) functionality providing audio services to calling parties. The IVR module works closely with the RADIUS server authentication, authorization and accounting. The IVR functionality features:

ANI/PIN Based Scripted Paths

SysMaster gateway provides predefined scripted paths for playing messages when the user dials in the gateway. Each call is first authenticated by ANI, and in the case that ANI authentication fails the, IVR Profile would be authenticated by PIN. Full audio services for PSTN and VoIP calls are supported, as well as post-paid and pre-paid accounts are fully supported. Through the interface, the SysMaster gateway can be programmed to only authenticate only by ANI or only by or fall back to both.

Pass-Through Functionality

SysMaster provides special Pass-through authentication based on tech prefixes. This mode is often used in tandem switching and PSTN switching. It can also be successfully used to switch VoIP to VoIP calls (2 IP legs are supported in one call). No audio services are supported. Post-paid and pre-paid accounts are fully supported;

Callback Functionality

SysMaster provides special IVR message paths to be played in connection with the way the user is authenticated/authorized.

Flexible DTMF Routing

The gateway allows for fine management of the DTMF message routing. It can selectively pass inband or out-of-band PCM16 frames. This can be suitable for cases when implementing Intelligent proxy or for peers supporting only certain type of DTMF routing. The system can enforce auto detection and intelligently select the right mode when no specific DTMF routing is required.

Language Servers

The SysMaster gateway allows for defining multiple language servers. Each server specifies an IVR server with a specific directory where audio file from the same language are located. This way administrators can easily switch between multiple languages. All language files should be first locally cached. This is done through the "Download Language Server"command, executed on each server.

Multiple Language Support

The IVR module allows administrators to give their users to select between two languages with an option. The selection message menu is played after initial dial into the gateway.

Multisession IVR

The SysMaster gateway can support multiple calls from an user that has already been authenticated by the system. In this way, the user can place easily multiple consecutive calls within one calling session. In order to this, the user simply has to press a predefined DTMF - usually this is "#".

Customer Service Redirect

This feature enables end users to quickly contact customer service representatives to discuss call issues or buy calling time over the phone. The system provides announcements to guide the users easily call through.

Calling Time/Balance Announcement

The IVR module can play the current balance of the user after he/she authenticates with the system. It can also selectively play the available calling time after the user has entered the destination number.

Pre-paid and Post-paid Account Support

All of the gateway features concerning user interaction are supported for both pre-paid and post-paid accounts.

Low Balance Announcement

The system can be configured to play a waning message when the balance is below a certain threshold.

IVR over IP

The SysMaster digital gateway can be used as a central point for RADIUS authentication/ authorization for IVR services to multiple analog gateways that do not have this functionality. All IVR messages are encoded over IP (using one of the selected endpoint codecs) and are transmitted to the remote analog gateway peer. On the other hand the analog gateway converts the announcements back to analog signal and plays them to the user.

Auto Attendant PBX Menu System

For the purposes of building a PBX IVR system, administrators can use the SysMaster gateway capabilities to construct arbitrarily deep levels of IVR menus. To this end, the gateway uses IVR Profiles and IVR objects which provide great flexibility. For more information, please refer to the IVR Objects section.

Intelligent Proxy

The Intelligent Proxy allows the VoIP Gateway to relay audio frames between H323 and SIP channels without using codec operations (encode/decode). This way, the gateway can achieve high call throughput. If the Intelligent Proxy does not operate, the gateway will always decode and encode the audio frames.

If Intelligent Proxy mode operates it can be enabled for any direction (receive or transmit) according to the following rules:

- the used codecs have CPU intensive encode/decode operations
- same audio codecs are used in both call legs. For this to work, SysMaster changes its codec preference order for outgoing calls and uses the peer's preference order for incoming calls. For H323 the Intelligent Proxy codec negotiations work better when Fast Start is used.
- if the used IVR Type is Pass-through Authentication or CDR Collection the Intelligent Proxy does not depend on the Inband DTMF Detection requirements.

IVR Profiles

Overview

Beside IVR information, IVR Profiles hold logic that determines the way IVR is played as well as the way authentication/authorization is done.

IVR Profiles are used for each Incoming Call. They are attached through the Inbound Profiles which are attached to an incoming call through a Call Filter.

When an IVR profile takes control over an incoming calls, the task of the VoIP Gateway is to perform authentication and authorization of the call using the selected RADIUS server. Next, the gateway has to play various IVR messages to the calling party, to determine the destination number, to call the VoIP routing to determine the endpoint to be used for the outgoing call according to the destination number and to bridge the audio traffic between the incomming call and the outgoing call.

Sometimes the IVR Profile does not instruct the gateway to play audio messages to the calling party. In this case, the gateway may directly connect both parties with no messgaes inbetween. This may the case when working in Proxy mode or in passthrough mode for PSTN-to-PSTN call termination.

Parameters:

Name	Specifies the name of the RADIUS server.
Type	Defines the type of the IVR Profile. IVR Profile types fully support VoIP switching (a call can come via IP and then be terminated via IP), as well as PSTN origination/ termination. Available IVR Profiles types are: ***ANI–*** designates that each call will be authenticated via ANI (Caller ID) type authentication. ***PIN*** -designates that each call will be authenticated via a PIN number. ***PIN / ANI*** - designates that each call will be first authenticated first ANI, and in the case that ANI authentication fails the IVR Profile would be authenticated by PIN. Full audio services for PSTN and VoIP calls are supported, as well as post-paid and pre-paid accounts are fully supported; ***CDR Only –*** designates that each call will be processed and routed without authentication. Final CDR records will be collected only. When CDR authentication is selected, no audio services will be supported. Post-paid and pre-paid accounts are fully supported; ***Pass-Thru –*** designates that each call will be authenticated via tech-prefix and then automatically routed. ***Two-Stage*** - each call will be processed and routed without authentication. RADIUS Server can be used for authorization if there is RADIUS Server Group specified; ***CallBack*** - each call will be rejected and data passed to Callback Server as a Call Back request. ***PBX*** - each call will be processed and routed without authentication. If there is RADIUS Server Group specified it will be used for CDR Collection.
Inband DTMF Detection	Specifies the status of the inband DTMF Detection to be used of PCM16 frames. Available options are: ***Yes –*** enables inband DTMF detection for PCM16 frames. ***No –*** disables inband DTMF detection for PCM16 frames. The option could be used when the peers send out of band DTMF tones or when the Intelligent Proxy is enabled. ***Auto/Both*** - detects inband and out of band DTMF ***Auto/OutOfBand*** - accepts only out of band DTMF.

Enable Intelligent Proxy	Specifies whether the Intelligent Proxy option would be activated or not. The Intelligent Proxy allows the VoIP Gateway to relay audio frames between H323 and SIP channels without using codec operations (encode/ decode).
Enable DTMF Relay To Leg 1	Allows for Leg 1 to receive DTMF tones. By default all DTMF tones received on Leg 2 are relayed to Leg 1.
Enable DTMF Relay To Leg 2	Allows for Leg 2 to receive DTMF tones. By default all DTMF tones received on Leg 1 are relayed to Leg 2.
Generate Artificial Ring Tones	When checked, artificial ring tones will be generated by the IVR profile.
Generate Connect Tone	When checked, connect tones will be generated by the IVR profile.
Language Server	Specifies an applicable Language Server. All files would be downloaded from the specified Language Server and would be played based on the IVR Selection.
Second Language Server	Specifies a Second Language Server only used if multi-language IVR is desired.
Enable Language Selection	Language Selection enables multi-lingual support. If checked, the gateway will play a prompt for language selection. The language files used would be the ones from the specified two language servers.
Enable Multisession IVR	Enables multi-session support. Multi-session allows multiple sequential calls from one account. (e.g. once the first call disconnects, the customer can initiate a second call, and so on).
Enable Customer Service Redirect	Enables Customer Service Redirect to the customer service phone number (listed below). The redirect can be done from any prompt level and will automatically connect the call based on the dial plan.
Customer Service Number	Specifies the customer service number that will be announced by the system. If the customer service number is dialed the caller will automatically be connected to the customer service representative.
Fist Digit Timeout (1-30 sec)	Specifies the time in seconds before the system times out and plays an error prompt message. The period of first digit timeout could be in the range from 1 to 30 seconds.
Digit Timeout (1-30 sec)	Specifies the time in seconds before the system times out and plays an error prompt message. The specified value could be in the range from 1 to 30 seconds.

PIN Length (1-20)	Specifies the maximum length of the PIN number. The PIN length could be specified in the range from 1 to 20 characters.
PIN Terminator	Specifies the PIN termination character. If the caller presses '#', or '*', or if the PIN timeout is reached, the PIN will be submitted. PIN terminator can be either an explicit character (#,*), or PIN entry timeout.
PIN Retries (1-5)	Specifies the maximum number of PIN entry retries that are allowed by the system. After the maximum number of attempts is reached the system will disconnect the caller.
Max Destination Number Length (1-40)	Specifies the maximum length of the called station number. This is the destination number that will be entered by the caller.
Destination Number Terminator	Specifies the Destination Number termination character. If the caller presses '#', '*', or if Destination Number timeout is reached, the Destination Number will be submitted. Destination number terminator can be either an explicit character (#,*) or destination number entry timeout.
Destination Disconnect	Specifies the character that allows multi-session call disconnect. Once this character is pressed, the current call will be disconnected and the system will prompt the caller for another call. This can be either an explicit character (#,*) or timeout.
Destination Number Retries (1-5)	Specifies the maximum number of Destination Number entry retries that are allowed by the system. After the number of attempts is reached the system will disconnect the caller.
Enable Number Redial	When checked, number redial will be performed.
Enable Pre-Paid Credit Message	Enables credit announcement for pre-paid callers.
Enable Post-Paid Credit Message	Enables credit announcement for post-paid callers.
Enable Pre-Paid Time Message	Enables credit time announcement for pre-paid callers
Enable Post-Paid Time Message	Enables credit time announcement for post-paid callers.
Enable Post-Paid Timer	Enables post-paid call timer (time based disconnect) for post-paid callers.

Drop Message Time (0, 10-60 sec)	Specifies the time before a warning disconnect message is played to the caller. If number entered is greater than 0 the message is enabled. If number specified is equal to 0 the message will be disabled. The system will announce to the caller that the call will be disconnected. The event will happen at the specified number of seconds before the actual call disconnect takes place.
End Message	Enables the end of call (good bye) message
Enable Recharge Account	Enables recharging of the account.
Recharge Threshold	Specifies the minimum balance threshold. If the balance is below the specified value the system will remind the caller with message.

Managing IVR Profiles

To Add IVR Profile

1. From the Navigation tree, select the **IVR Management > IVR Profiles** node.
2. From the Edit Menu select 'Add IVR Profile'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the modifications.

To Edit IVR Profile

1. From the Navigation tree, select the **IVR Management > IVR Profiles** node.
2. From the right pane of the Navigator, select the IVR Profile to be edited.
3. From the Edit Menu select 'Edit IVR Profile'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce the modifications.

To Delete IVR Profile

1. From the Navigation tree, select the **IVR Management > IVR Profiles** node.
2. From the right pane of the Navigator, select the IVR Profile to be deleted.
3. From the Edit Menu, select the Delete menu item.

IVR Objects

Overview

IVR objects serve to build custom menus for the PBX system. They are attached to IVR profiles. IVR objects consist of user selection filter, pointers to audio files to be played, and action to be taken over the call (dialing, a number, dropping the call, connecting to other menu etc). They allow for building multilevel menus. Each menu object should be constructed from files having the same prefix and delimited with "." e.g. menu.1, menu.2 ... menu.N.

Parameters:

Path Name	Defines the name of the menu.
Selection	Specifies the digit used to select the menu entry.
Anouncement Audio File Name	Specifies the name of the audio file to use. This name together with the language abbreviation and the audio format specifies the name of the file in use.
Selection Audio File Name	Specifies whether the Intelligent Proxy option would be activated or not. The Intelligent Proxy allows the VoIP Gateway to relay audio frames between H323 and SIP channels without using codec operations (encode/ decode).
Action	Specifies the action that will be performed if the selection is matched. There are several actions that can take place: ***Dial*** ***None*** ***Drop Call*** ***Directory Dial*** ***Enter Path*** ***Exit Path***
Advanced Rule	Specifies the Advanced Rule to be applied to the Call Filter. Advanced Rules allow for flexible enforcement of the call filter based on time or endpoint availability.

Managing IVR Objects

To Add IVR Object.

1. From the Navigation tree, select the **IVR Management > IVR Objects** node.
2. From the Edit Menu select 'Add IVR Object'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce the modifications.

To Edit IVR Object.

1. From the Navigation tree, select the **IVR Management > IVR Objects** node.
2. From the right pane of the Navigator, select the IVR Object to be edited.
3. From the Edit Menu select 'Edit IVR Object'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce the modifications.

To Delete IVR Object.

1. From the Navigation tree, select the **IVR Management > IVR Objects** node.
2. From the right pane of the Navigator, select the IVR Object to be deleted.

3 From the Edit Menu, select the Delete menu item.

Language Servers

Overview

Language Servers are used to store audio files through which the IVR logic will assemble audio messages, e.g. announcing numbers, text messages and prompts. To this end, a Language Server is pointed to in the IVR Profile. A Language Server actually represents a directory on a remote server (TFTP protocol server) where audio files are stored. The SysMaster gateway can also store locally multiple audio files. Each audio file has a name defined by a short designation of the language as well as a part determining the type of message it holds.

Each Language Server is identified by name. Remote Servers additionally designate remote hosts with IP addresses and directories from where audio files are downloaded only one time upon administrator's request. Thus, two remote language servers can even use one and same directory name, but the difference comes from the file name prefix of the files determining the language of the files. This feature is especially helpful for TFTP servers that can have only one publicly available directory.

On the other hand, Local Language servers do not use IP addressees, directory or Timeouts. Their audio files are uploaded in one directory and are installed (i.e. activated) only when required.

The download of the audio files from remote servers is (in different formats) performed by a specified protocol (TFTP or HTTP). The actual download procedure is done manually by the administrator of the gateway. Using the Sysmaster Console Navigator, administrators should go to **Language Servers > Language Servers > [Language Server item]** and from the menu select the "Download Language Server" menu command.

Depending on the Language Server type (Remote/Local), the following operations can be performed:

- File Name change (all type of Language servers).
- Change of the Audio File contents
  Each file can be uploaded and overwritten as well as played back.
- Adding new files
  This allows for adding more files outside of the objurgatory files on which the IVR functionality relies.

Each audio file has its status. For Remote Language Servers it can be:

- New - the file has never been downloaded;
- Failed - the system has decided that the file has not been downloaded correctly or that the download has failed entirely;
- Downloaded - the file has been successfully downloaded.

For Local Language Servers it can be:

- New - the file has never been uploaded;
- Not uploaded - the file has not been successfully uploaded;
- Uploaded - the file has been successfully uploaded.

The purpose of all operations on both Local and Remote Language servers is for the IVR logic to find installed files of one Language Server in one directory.

Parameters:

Name	Defines the name of the language server that stores the audio files.
Protocol	Specifies the protocol to be used by the Language Server Available protocols are: ***TFTP*** ***HTTP***
IP Address	Assigns an IP address to the Language Server
Directory	Designates the directory within the Language Server where audio files would be stored. The directory should be named after the language abbreviation of the audio files being stores in it. (e.g. 'en' for English, 'fr' for French, 'sp' for Spanish, etc) located in.
Timeout (1-60)	Defines the period of time (in seconds) for timeout of the server query. Language server timeout could range from 1 to 60 seconds.
Language	Specifies the index (language abbreviation) of the audio files located in the language server. When naming audio files the following convention should be used: <index_file.au> , where index is the language abbreviation for the audio file. Foe example, the file en_welcome.au would store the customized welcome message in English.
File Format	Specifies the format of the IVR files stored in the Language Server. The selections available are: ***PCM - uLaw 8kHz (.au)*** ***GSM (.gsm)***

Language Type	Defines the type of the Language Server. Available options are: ■ Regular - file "md_and" is not used and numbers are said like in English. ■ All Join - file "md_and" is played between every major digits (20,30,...100,...1000) and "one" in one hundred and one thousand is skipped. ■ Last Join - file "md_and" is played after last major digit and "one" in one hundred and one thousand is skipped.
Description	Allows a short description (up to 71 characters) of the conference profile to be entered.

Managing Language Servers

To Add Language Server.

1. From the Navigation tree, select the **Language Server > Language Servers** node.
2. From the Edit Menu select 'Add Language Server'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce modifications.

To Edit Language Server.

1. From the Navigation tree, select the **Language Server > Language Servers** node.
2. From the right pane of the Navigator, select the Language Server to be edited.
3. From the Edit Menu select 'Edit Language Server'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce modifications.

To Delete Language Server.

1. From the Navigation tree, select the **Language Server > Language Servers** node.
2. From the right pane of the Navigator, select the Language Server to be deleted.
3. From the Edit Menu, select the Delete menu item.

To Download Files of a Language Server.

1. From the Navigation tree, select the **Language Server > Language Servers** node.
2. From the right pane of the Navigator, select the Language Server whose files will be downloaded.
3. From the Navigator menu, select the Download Language Server.

Language Server Files

Overview

Each Language Server file contains a piece of audio message. The IVR functionality of the gateway uses these audio files to assemble longer messages such as numbers, text messages, prompts etc. Language Server Files are organised in Language Servers that can be either Local or Remote.

The format of the files should be one the following:

- PCM - uLaw 8kHz - use ".au" extension;
- GSM - use ".gsm" extension.

For more information, please refer to the Language Server section.

Parameters:

File Name	Specifies the name of the audio file to be uploaded. The name would be used as part of the file name for the audio file. For example, entering a name of 'welcome' would result in a file name 'en_welcome.au'.
Description	Specifies a Second Language Server only used if multi-language IVR is desired.

Managing Language Server Files

To Add Language Server File.

1. From the Navigation tree, select the **Language Server > Language Server Files > [Language Server]** node.
2. From the Edit Menu select 'Add Language Server'.
   A dialog box shows up.
3. Fill in the data and click on the Apply button to enforce modifications.

To Edit Language Server File.

1. From the Navigation tree, select the **Language Server > Language Server Files > [Language Server]** node.
2. From the right pane of the Navigator, select the Language Server File to be edited.
3. From the Edit Menu select 'Edit Language Server'.
   A dialog box shows up.
4. Fill in the data and click on the Apply button to enforce modifications.

To Delete Language Server File.

1. From the Navigation tree, select the **Language Server > Language Server Files > [Language Server]** node.
2. From the right pane of the Navigator, select the Language Server File to be deleted.
3. From the Edit Menu, select the Delete menu item.

To Listen To a Language Server File.

1. From the Navigation tree, select the **Language Server > Language Server Files > [Language Server]** node.
2. From the right pane of the Navigator, select the Language Server File to listen.
3. From the Edit Menu, select the Listen To Downloaded File menu item.
4. A dialog will popup to download the file. Click on the Save button.
5. Locate the saved file and play it in your favorite audio player supporting ".wav" files.

Chapter 9 PBX Server

Overview

The document describes key provisioning issues related to the configuration of the SysMaster PBX Server under the SM 7000 Platform.

SysMaster PBX server configuration involves:

- Call Filter Configuration
- Inbound Profile Configuration
- PBX Group Configuration

The components above also depict the basic call flow for processing of calls by the SysMaster PBX server.

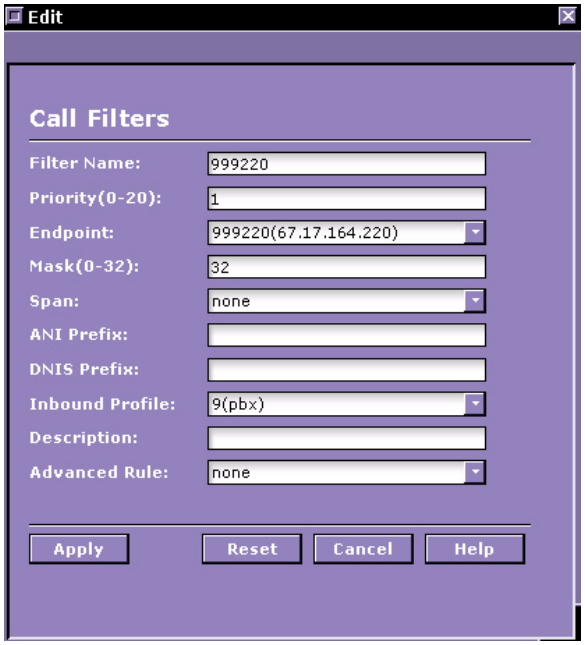
The following sections provide basic explanation and interconnectivity guidelines for each of the configuration tasks above.
Special importance will be given to PBX Groups and PBX Extensions configuration. For more detail explanation on the rest, please refer to the corresponding chapters of the user manual.

Call Filter Configuration

Call Filters could be viewed as firewalls granting or denying access to incoming calls. When an incoming call is accepted the call will be associated with an inbound profile.

In turn, the inbound profile will specify a set of parameters according which the PBX server will handle incoming calls.
Call Filters are the first processing component of the PBX Call Flow but the last to be configured within the actual PBX work flow.

A sample PBX Call Filter configuration could be:



Upon Call filter configuration special attention should be played to the selection of the following components:

- Endpoint
- Inbound Profile

For more detail information on how to set up call filter, please refer to **Chapter 3 "Call Processing"** of the user manual.

Inbound Profile Configuration

For the purpose of this document, an Inbound Profile specifies how the PBX incoming call will be handled once accepted by the call filter.
Important parameters that could be designated within an Inbound Profile are:

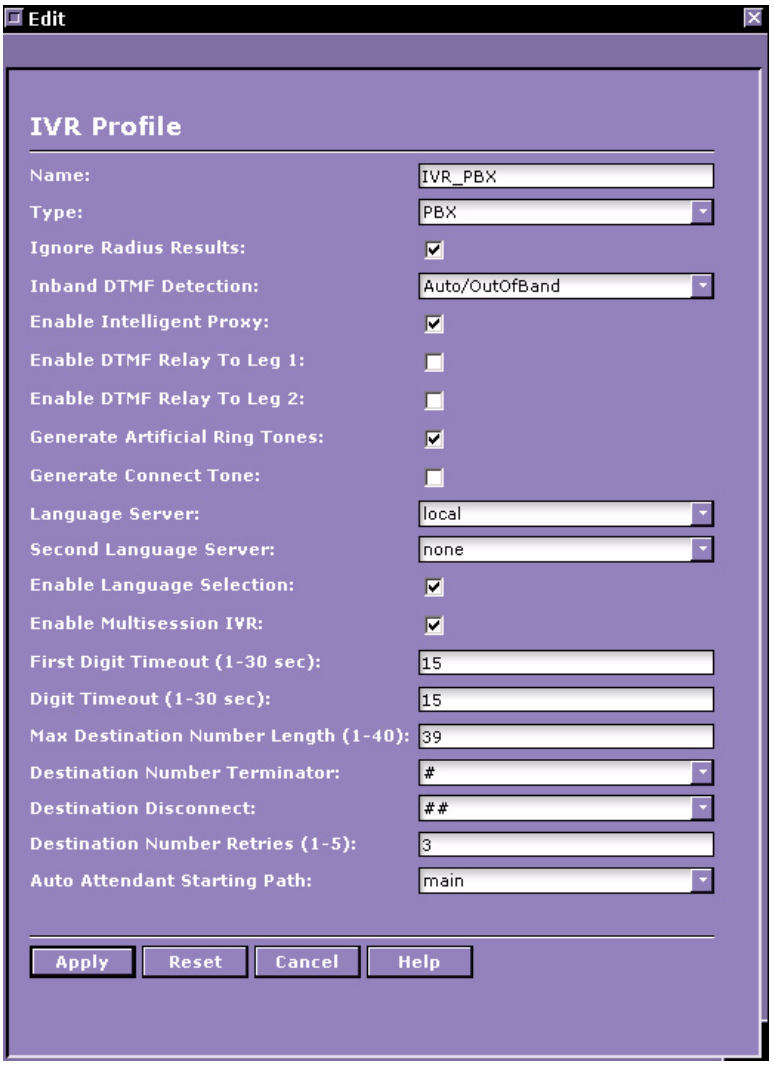
- IVR Profile Type
- Routing Table Type
- PBX Group Type

The IVR Profile Selected will contain the proper IVR logic that will be played on the side of the PBX. Also an IVR Profile of type PBX is the place where the enhanced Auto Attendant logic should be input.
The SysMaster Auto Attendant allows easy definition of complex PBX menus and sub-menus to be achieved.
Keeping within the tone of this section, next we will describe how to create IVR Profiles for servicing the SysMaster PBX Server. In addition, IVR Objects will also be discussed.

An IVR Profile is associated with an incoming call through the Inbound Profile attached to

the designated Call Filter.
Each IVR Profile created is characterized by its type. Thus, the first step in configuring an IVR Profile is selecting an appropriate IVR type. In our case, the IVR Profile will be of type PBX.

A sample PBX type IVR Profile configuration is depicted below:



The value of the last field (Auto Attendant Starting Path) selected establishes the connection between an IVR Profile and an IVR Object.

IVR Objects are used for tuning up the Auto Attendant feature of the PBX Server. In other words, IVR Objects are used for building customized menus and sub-menus for the SysMaster PBX Server. They are attached to the IVR Profile through the Auto Attendant Starting Path. Visually, an Auto Attendant Starting Path could be conceived as a container in which you can arrange different menus and submenus.
For example, we wish all menus or submenus to be within a single container called **main.** Each menu and submenu will correspondent to a single IVR Object and be responsible for the announcement of separate greetings. (**i.e**. Welcome to the PBX System, For sales press 1, For support press 2, etc)

The way we can put all menus and submenus within the single **main** container is by giving them appropriate names. That is, the fist part of the name should consist of the name of the container (in our case **main**) and the second one, preceded by a dot ì.î , should be the arbitrary name given to the menu/sub-menu. (**e.g.** main.1; main.2; main.N1; main.N2)

In addition, an IVR Object or sub-menu could contain two types of prompts: non-action or action prompts. A non-action prompt is comprised only of a single Announcement Audio File that should be specified upon IVR Object configuration.

An action prompt on the other side contains an Announcement Audio File, a selection audio file and a type of action attached to it.
The following IVR Object actions are available:

- Dial
- Drop Call
- Directory Dial
- Enter Path
- Exit Path
- Repeat Menu
- Dial To Conference
- Dial To Follow Me
- Dial To ACD
- IVR Function
- Switch To

The action selected will be triggered each time the IVR Object is played and after a user has made a selection.

An action prompt IVR Object is played in the following manner:

1. Announcement Audio File is played
2. User makes a selection

PBX Group Configuration

A PBX Group represents a blueprint outlining the basic behavior of all PBX extensions contained within it and at the same time allows configuration of global PBX parameters

A PBX Group is identified by the following set of parameters:

Name	Specifies the name of the PBX Group. The name could contain any combination of alphabetical and numerical characters.
Status	Indicates whether the PBX Group created is enabled or disabled. When disabled status is selected the PBX Group would not function even though it has been defined.

First Park Number	Allows the user to "park" a call at the specified number, and access (dial) the "park" number through another phone on the system to retrieve the call.
Last Park Number	Specifies the last park number needed for establishing a range within which the feature would operate. The starting point of the range is the specified First Park Number.
Parking Timeout	Specifies the maximum time (in seconds) for which a call can operate in the "park" mode.
IVR Profile	Specifies the default IVR Profile that will be used by the PBX Group.
Default Route	Specifies the Default Routing table that will be used by the PBX Group

There are several types of actions that could be configured within a PBX Group:

- Call Parking
- IVR Profile Connectivity
- Default Route Connectivity

Call Parking

SysMaster 7000 GW provides a flexible way for conducting call park of calls.
Call park allows you to place a call on hold, by specifying a call park extension range, and later retrieve it from another phone. For example, if a user dials a phone number that is currently active, the receiving end can ìparkî the call to a call parking extension (i.e. 122) and then the parked call could be retrieved by another phone on the system by dialing the call parking extension specified.

To achieve such a scenario, you need to specify a range of call park numbers that will be used as extensions. A call park range is defined by the first park number and last park number specified.

IVR Profile Configuration

A PBX Group should be associated with an IVR Profile in order proper IVR logic to be played. The IVR Profile selected should be the same as the one created under IVR Profiler configuration.

IVR Profiles are attached to a PBX Group by simply selecting the proper profile from the list of available ones.

Default Route Configuration

Default Route Configuration joins a PBX Group to an existing route on the system, thus ensuring proper routing of calls. Routes are configured through the custom route window under **Call Routing > Routes > Add Custom Route**.

For detailed information on route configuration refer to **Chapter 6 "Call Routing"** of the user's manual.

Managing PBX Groups

To Add PBX Group

1. From the Navigation tree, select the **PBX > PBX Groups** node.
2. From the Edit Menu select 'Add PBX Group'
   A dialog box shows up.
3. Fill in the data, and click on the Apply button to enforce the modifications.

To Edit PBX Group

1. From the Navigation tree, select the **PBX > PBX Groups** node.
2. From the right pane of the Navigator, select the PBX Group to be edited.
3. From the Edit Menu select 'Edit PBX Group'.
   A dialog box shows up.
4. Fill in the data, and click on the Apply button to enforce modifications.

To Delete PBX Group

1. From the Navigation tree, select the **PBX > PBX Groups** node.
2. From the right pane of the Navigator, select the PBX Group to be deleted.
3. From the Edit Menu, select the Delete menu item.

PBX Extensions

Once a PBX Group has been created, PBX Extensions could be added to it. All PBX Extensions will inherit the default behavior of the group they belong to.

A PBX Extension is associated with a single party within a PBX Group. One or more PBX Extension could be contained within a group.

PBX Extension parameters that could be configured are:

Directory Name Dialing Initials	Directory Name Dialing Initials allows in-bound callers to have their calls routed to the appropriate person without having to enter the person's extension number. Once implemented the feature will conduct a first and last name directory look up and determine the appropriate party to receive the call. The only setting that needs be specified is the value of the Directory Name Dialing Initials field. In it you can enter the first or last name of the party that will participate in the directory name look up.

Status	The Status flag serves as an indicator of whether a PBX Extension is operational or not. Selecting a Status Enabled ensures that the PBX Extension is active, where status disabled indicates that a PBX Extension has been created but is still not functional.
Enable DND	When checked DND (Do Not Disturb) will be enabled. The functionality allows you to block incoming calls from ringing the terminal. Once enabled the DND feature will trigger either a call forward of the blocked incoming number or a transfer of the incoming call to the specified voicemail number below. For more information refer to the Forward and Voicemail Number field explanations.
Hide Caller ID	When selected the Caller ID of the calling party will not be displayed.
Enable Call Waiting	When checked call waiting will be enabled.
Enable Call Screening	The option activates Call Screening.
Enable Call Recording	When selected the Caller ID of the calling party will not be displayed.
Forward	Call Forward is used in conjunction with the DND functionality. Call Forward specifies a set of conditions for which forwarding of calls will be enabled. Available conditions are: ■ If Busy/No Answer ■ If Busy ■ If No Answer Call Forward will be triggered once the selected condition has been met.
Forced DND Rule	The option allows you when the enabled DND Rule will take effect. The field allows you to enter a number to which calls will be forwarded. Call forwarding will be enabled based on the forward rule specified. The option will allow you to enter a new number based on the DND rule selected. The field allows you to enter a number to which calls will be forwarded. Call forwarding will be enabled based on the forward rule specified. The field allows you to enter a number to which calls will be forwarded. Call forwarding will be enabled based on the forward

Forward Number	The option allows you to specify a forward number that calls will be redirected to in case the PBX Extension is unavailable. Number forward is processed based on the Forward rule selected above.
Voicemail Number	The option allows you to specify a voicemail number that calls will be redirected to.
Speed Dials	Speed dial is used for faster dialing of numbers. The feature allows administrators to create system level dial codes that can be used by any telephone terminal connected to the PBX. For enabling speed dial capabilities two sets of numbers must be defined (e.g. 1 = 1221843553). The number to the left of the equal sign denotes the speed-dial number that needs to be called. The number to the right is the phone number to be replaced by the speed dial number.
Timeout	In the event that a PBX Extension is not reachable, the system will periodically initiate a query trying to locate the PBX Extension. The time the PBX Extension query will be initiated for is controlled by the value of the Timeout field. Once the timeout is reached, the system will cease initiating the PBX Extension query.

Managing PBX Extensions

To Add PBX Extensions

1. From the Navigation tree, select the **PBX > PBX Extensions > [PBX Extension]** node.
2. From the Edit Menu select 'Add PBX Extension'
   A dialog box shows up.
3. Fill in the data, and click on the Apply button to enforce the modifications.

To Edit PBX Extensions

1. From the Navigation tree, select the **PBX > PBX Extensions > [PBX Extension]** node.
2. From the right pane of the Navigator, select the PBX Extension to be edited.
3. From the Edit Menu select 'Edit PBX Extension'.
   A dialog box shows up.
4. Fill in the data, and click on the Apply button to enforce modifications.

To Delete PBX Extensions

1. From the Navigation tree, select the **PBX > PBX Extensions > [PBX Extension]** node.
2. From the right pane of the Navigator, select the PBX Extension to be deleted.
3. From the Edit Menu, select the Delete menu item.

To Delete All PBX Extensions

1. From the Navigation tree, select the **PBX > PBX Extensions** node.
2. From the Edit Menu, select the Delete All menu item.

Chapter 10 Voice Mail Server

Introduction

Overview

GW 7000 supports H323, SIP and PSTN protocols to allow flexible call processing. Callers can connect to the Voice Mail platform via IP or PSTN or Web and have full access to all advanced Voice Mail functionality. International and long-distance VoIP callers can also leave, retrieve, and manage messages in real-time from a remote Voice Mail server. In addition, the platform allows telecommuters and corporate field associates to take advantage of Voice Mail functionality while traveling or working from remote locations. GW 7000 unique features flexible price structure and high return on investment.

Features

- Unlimited Number of Mailboxes
- Long-distance and International Voice Mail Support
- H323,SIP and PSTN Protocol Support
- Complete Voice Mail Functionality over IP and PSTN
- Password/PIN Based security
- Web and Phone Management Access for Mailbox Users and Administrators
- Voice Mail Email Exchange and Notification
- Voice Mail Forwarding
- RADIUS Billing Interface
- Managed Services and Virtual Platform Partitioning Support

Unlimited Number of Mail Boxes

GW 7000 supports an unlimited number of mailboxes with pre-set size quotas. The mailboxes are grouped for flexible administrative templates and easy management mailbox users can also be related to PBX accounts to allow single access to PBX and Voice Mail functionality.

Long-Distance and International Voice Mail

GW 7000 allows long-distance and international users to support virtual mailboxes outside the country of their residence. In fact users can be anywhere in the world and retrieve their messages via Web, Email, or VoIP. This allows extremely flexible platform implementation and dynamic virtual office support.

H323, SIP, PSTN/TDM Web, Email Access Support

GW 7000 allows callers to leave a message for unavailable users once they connect to the platform via VoIP or PSTN. In addition, users can manage their greetings or passwords via VoIP or PSTN as well. The messages can be retrieved via Web, VoIP, PSTN, and Email to allow flexible mailbox management and low retrieval cost.

Web and Phone Mailbox Management

GW 7000 allows flexible mailbox management for all system users to provide them with the necessary tools to modify greetings and passwords, to delete and forward messages, and to setup mailbox options. Administrators can expire, lock, and restrict user accounts to secure the system integrity.

RADIUS Billing Interface

GW 7000 supports Radius Billing Interface to SysMaster VM2000 Billing Platform. This allows the Voice Mail server to support real time billing procedures where as all inbound voice mail messages are accounted and billed for.

Voice Mail Groups

Parameters:

Group Name	Specifies the name of the voice mail group to be added.
Group Status: Enable / Disable	Verifies the password.
Max Messages	Specifies the maximal number of voice messages contained within the group.
Max Message Time	Specifies the maximal duration of the message in seconds.
Lock Attempts	Allocates a number for the lock attempts to be performed.
Audio Format	Specifies the audio format of the voice mail file.
Quick Menu	Specifies whether a quick menu will be included in the created voice mail group.
Enable Administration	If checked, remote administration could be performed.
Authentication Method	Specifies how the voice mail group would be authenticated.
RADIUS Group	Specifies the Radius Server Group of the Radius Server to use
Description	Allows a short description (up to 71 characters) of the conference profile to be entered

Managing Voice Mail Groups

To Add Voice Mail Group

1. From the Navigation tree, select the **Voice Mail > Voice Mail Groups** node.
2. From the Edit Menu select 'Add Voice Mail Group'
   A dialog box shows up.
3. Fill in the data, and click on the Apply button to enforce the modifications.

To Edit Voice Mail Group

1. From the Navigation tree, select the **Voice Mail > Voice Mail Groups** node.
2. From the right pane of the Navigator, select the Voice Mail Group to be edited.
3. From the Edit Menu select 'Edit Voice Mail Group'.
   A dialog box shows up.
4. Fill in the data, and click on the Apply button to enforce modifications.

To Delete Voice Mail Group

1. From the Navigation tree, select the **Voice Mail > Voice Mail Groups** node.
2. From the right pane of the Navigator, select the Voice Mail Group to be deleted.
3. From the Edit Menu, select the Delete menu item.

Voice Mail Boxes

Parameters:

Box Name	Specifies the name of the voice mail box to be configured.
Extension Number	Denotes the extension number to be used for accessing the Mail Box.
Email	Specifies the email of the administrator administering the Mail Box.
Attach Message to Email	Specifies the maximal duration of the message in seconds.
Client Name	Identifies the user name to be used upon administering the Mail Box.
Password	Assigns a password necessary for accessing the Voice Mail Box.
Confirm Password	Confirms the password entered above.
Password Expiration	Specifies the expiration period for the Voice Mail Box password. After the end of the expiration period the assigned password will no longer be valid and a new one must be specified.

Mail Box Expiration (days)	Specifies the expiration period for the Voice Mail Box. After the end of the expiration period the Voice Mail Box will no longer be active.
Box Status	Enables or disables the current Voice Mail Box.
Web Management	Enables Web Management.
Email Management	Enables Email Management. When enabled Email Management would allow messages to be attached to emails sent to the address specified in the email field.
Custom Announcement	Enables custom announcements.
Locked	When checked the Voice Mail Box would be locked.
Disable "Delete"	When checked users will not be able to manually delete messages contained within a Voice Mail Box.
Disable "Delete All"	When checked users will not be able to manually delete all messages contained within a Voice Mail Box.
Disable "Delete Forwarded"	When checked users will not be able to manually delete forwarded messages contained within a Mail Box.
Voice Mail Group	Associated the Voice Mail Box with an already created Voice Mail Group.

Managing Voice Mail Boxes

To Add Voice Mail Box

1. From the Navigation tree, select the **Voice Mail > Voice Mail Boxes** node.
2. From the Edit Menu select 'Add Voice Mail Box'
   A dialog box shows up.
3. Fill in the data, and click on the Apply button to enforce the modifications.

To Edit Voice Mail Box

1. From the Navigation tree, select the **Voice Mail > Voice Mail Boxes** node.
2. From the right pane of the Navigator, select the Voice Mail Box to be edited.
3. From the Edit Menu select 'Edit Voice Mail Box'.
   A dialog box shows up.
4. Fill in the data, and click on the Apply button to enforce modifications.

To Delete Voice Mail Box

1. From the Navigation tree, select the **Voice Mail > Voice Mail Boxes** node.
2. From the right pane of the Navigator, select the Voice Mail Box to be deleted.
3. From the Edit Menu, select the Delete menu item.

Chapter 11 Callback Server

Overview

The SysMaster gateway can act as a callback server. A callback server operates the following way:

1. A user sends to the gateway a PIN, a source number (the number from which the user wants to place a call) and destination number through a web request, email, or SMS message.
2. Next the call back server authenticates the user, calls back to the source number that the user has provided and at the same time calls the destination number. This way the gateway connects both parties. Alternatively, the destination number can be provided later after the gateway calls back the user first. Then the user will hear an IVR message prompting him/her to enter the destination number.

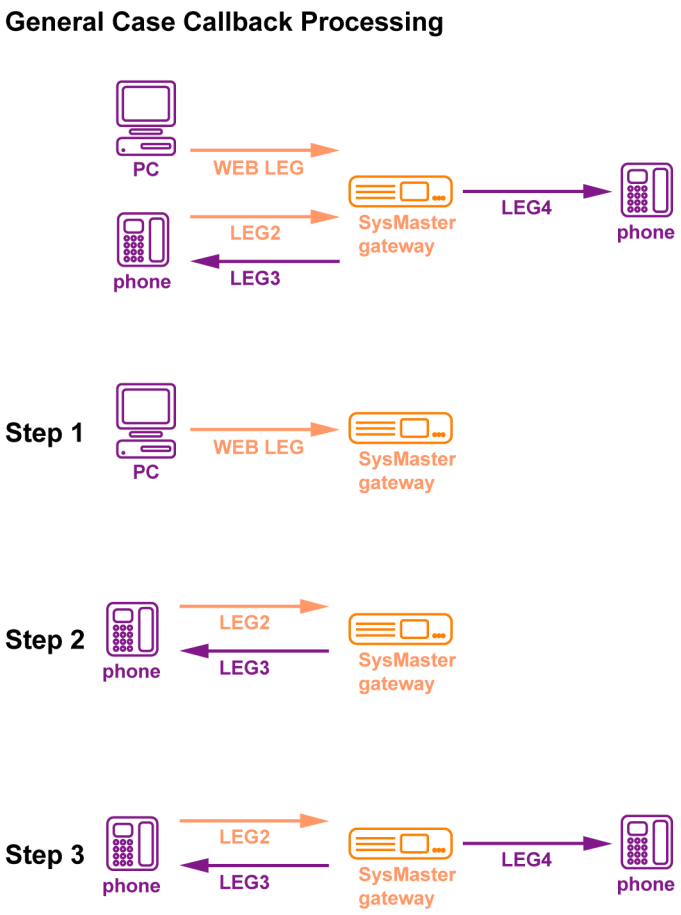
The callback server can receive requests from:

- Web based HTTP request
- SMS messages
- Email messages
- PSTN calls (ANI authentication/DID)

There are two ways of authentication:

- PIN based authentication (web callback, email callback, sms callback)
- ANI (Caller ID, source number)/DNIS based authentication (PSTN callback)

General Callback Server Processing



The general operation of the callback server includes the following steps:

1. The gateway receives PIN, prefix, source number and destination number through the web interface or SMS or email. The prefix and destination number are optional. If the destination number is omitted, it should be later provided.
2. (Step 1) Upon receiving the callback request, the gateway internally creates an incoming call leg with the following parameters:
   ANI[web] - source number.
   DNIS[web] - destination number

   According to the values above:
   ANI[web] = 12315101234567
   DNIS[web] = 22201234567
3. The gateway intercepts the internally created incoming call with a Callback filter that matches against the callback server endpoint. The primary Call Filter must have higher priority than the secondary Callback Filter (Callback filters should be created in pairs) so that it takes call processing control. The primary Call Back filter should redirect to an already created Inbound Profile.

4 Next the call is processed by the selected Inbound profile of the primary Call Filter. It does the following:
- The system will perform RADIUS authentication based on the submitted PIN number.
- The system strips the ANI[web] from any prefixes so that it can have the number ready for call routing followed with call setup to the origination party. The stripping pattern should be "prefix=" and according to the values of the example it should be "123=", thus the number submitted for call routing will be 1511234567.
- Next, the gateway performs routing to resolve the endpoint it use to setup call with the origination party, as indicated by the source number (1511234567).

5 At the time the gateway calls the origination party, the gateway creates a call leg to the origination party (LEG2) and a call leg from the origination party to the gateway (LEG3). In this case LEG2 is outgoing and LEG3 is incoming.
LEG2 (Step 2) includes the following parameters:
ANI[LEG2] - the Caller ID of the gateway
DNIS[LEG2] - coincides with the stripped ANI[WEB], i.e. 15101234567

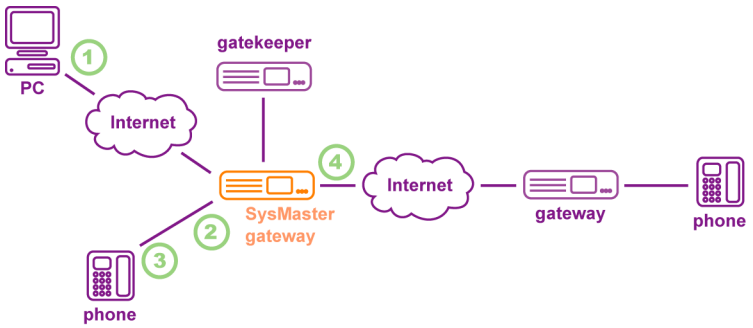
LEG3 (Step 3) includes the following parameters:
ANI[LEG3] - coincides with the nonstripped ANI[WEB], i.e. 12315101234567
DNIS[LEG3] - coincides with the prefix + DNIS[WEB], i.e. 12322201234567

6 After the gateway calls the origination party, it will play IVR messages to the origination party according to the IVR profile selected in the Inbound profile. If the user did not specify a destination number, the system will prompt him/her to enter the destination number.

7 Next the call is processed by the selected Inbound profile of the secondary Call Filter. It does the following:
- The system will perform RADIUS authentication based on the submitted PIN number.
- The system strips the DNIS[LEG3] from any prefixes so that it can have the number ready for call routing to the destination party. The stripping pattern should be "prefix=" and according to the values of the example it should be "123=", thus the number submitted for call routing will be 22201234567.
- Next, the gateway performs routing to resolve the endpoint it should use to setup a call with the destination party, as indicated by the destination number (22201234567)
- While waiting for the gateway to connect through to the destination party, the gateway will play IVR messages to the origination party according to the IVR profile selected in the Inbound profile.
- The gateway performs any additional ANI/DNIS translations if such are provided in the outbound profile of the selected routing table.

8 The gateway connects to the destination party by creating outgoing LEG4. When the destination party picks the call then both parties are finally connected.

Web Initiated Callback Services



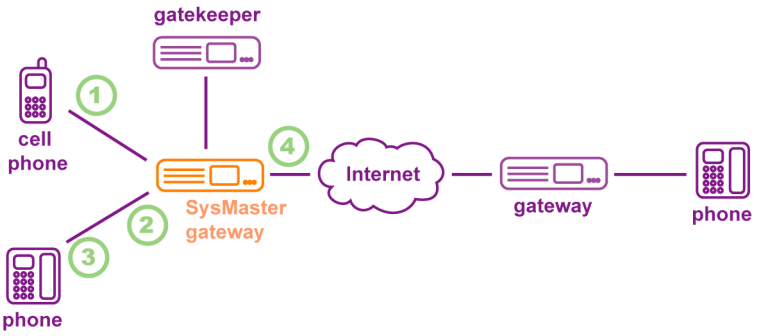
The Web based callback server uses PIN authentication. It operates in the following way:

Let's suppose the DNS with which the gateway is configured is www.callback.com and that the gateway is visible on the Internet. Using a computer connected to the Internet, a user sends an HTTP callback request using the following URL: (the IP address below is provided as an example only)

http://192.168.0.154/cb

SysMaster GW authenticates the user and calls back to the registered phone number.

SMS Initiated Callback Services



The SMS callback server uses PIN authentication. The SMS based callback server operates in the following way:

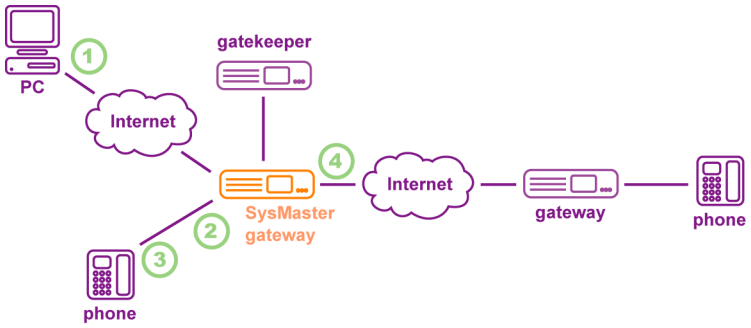
1. A user sends an SMS message by dialing into the gateway using the SIM number of the gateway
2. The user enters the PIN, prefix, source number, destination number in the following format:

   PIN
   prefix (optional)

source number
destination number (optional)

3 The gateway processes the callback request following the general callback procedure

Email Initiated Callback Services



The Email based callback server uses PIN authentication. It operates in the following way:

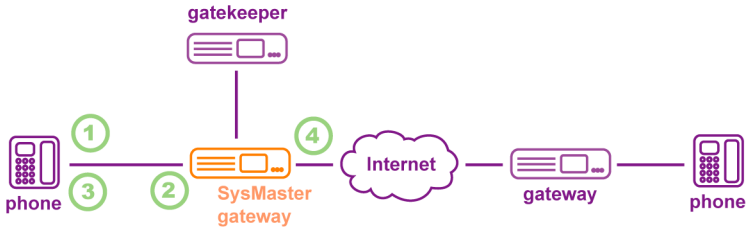
1 A user sends an email message to the SMTP server running on the gateway. The email address is as specified in the **System Configuration > Callback Server** node.

2 The user enters the PIN, prefix, source number, destination number in the following format:

PIN
source number
destination number (optional)

3 The gateway processes the callback request following the general callback procedure

Phone Initiated Callback Services



This is a method for authenticating users based on ANI (Caller ID) or DNIS.

1 A user dials into the SysMaster gateway using dial-in gateway number. After establishing connection the user should hang up after he/she hear a busy signal.

2 The gateway contacts the RADIUS server to authenticate the user based on the ANI or DNIS (based on the number the calling party used to dial into the gateway). If the

authentication is completed, the RADIUS allows the gateway to continue with the callback procedure.

3 The gateway places a call to the ANI number and prompts the user (by IVR message) to dial the desired destination number.

General Callback Parameters

Following is a list of the SysMaster callback server:

Callback Server Status: Active / Inactive	Specifies the Callback Server Status. The Callback Server functionality could be manually activated or deactivated.
Request Retry	Specifies time interval in seconds between two consecutive callback requests coming from the same IP address.
Request Time Threshold	Specifies the time within which the request should be placed. Otherwise it is rejected.
Callback Delay (5-600 sec)	
Redirect Mode: Local Server / Remote Server	Specifies the Redirect Mode of the Callback Server. When Local Server redirect mode is selected, Callback Server requests would be delivered locally. Remote Server redirect mode indicates the requests would be redirected to a remote server.
Redirect Server	Specifies the IP address of the Redirect Server when Remote Server redirect mode is enabled.
SMS Status: Active / Inactive	Specifies whether the callback server can process requests coming from SMS.
ANI Status: Active / Inactive	Specifies whether the Callback server can use its caller ID when placing the calls
SIM PIN	Specifies the SIM PIN number which the gateway will use to authenticate to the GSM network.
SIM Number	Specifies the SIM Number which is the gateway DNIS number.
Email Status: Active / Inactive	Email Status specifies whether the gateway callback server will process requests initiated from email.
Email Address	Specifies the email to which callback requests should be sent.
SMTP Listen IP Address1	Specifies the first SMTP Listen IP address at which the gateway's SMTP server will receive email messages.
SMTP Listen IP Address2	Specifies the second SMTP Listen IP address at which the gateway's SMTP server will receive email messages.

CallBack Server Setup

To configure the callback server, make sure you have configured the system in the following way (see next page):

Managing Callback Server Setup

To Edit Callback settings

1. From the Navigation tree, select the **System Configuration > Callback Server** node.
2. From the right pane of the Navigator, select the System User to be edited.
3. From the Edit Menu select 'Edit Settings'.
   A dialog box shows up.
4. Edit the callback settings to set its operational parameters. Click on the Apply button to complete the setup.

Chapter 12 Conference Server

Introduction

H323, SIP and PSTN Support

SM7000 Conference Server supports H323, SIP, and TDM protocols to allow all types of callers to connect to the conference server. In addition it supports IVR over IP for flexible user authentication and system interaction. Utilizing VoIP and PSTN based access methods the platform significantly increases the system performance and reduces the cost associated with local and long-distance call management.

One and Two-Stage Dialing

SM7000 supports one and two-stage conference profiles. The one-stage profile allows the callers to enter a conference room number associated with a dedicated DID number. The one-stage conferencing reduces the number of steps to enter a virtual conference room number. The two-stage profile allows the callers to enter a virtual conference room number once they connect to the system via a universal DID number. This procedure allows the platform manager to support a single DID access number and allow the callers to dial a virtual conference room number once they are connected.

Conference PIN Authentication

SM7000 supports PIN based authentication for all callers as well as the conference room administrator. The callers may be asked based on the conference profile settings, to provide PIN in order to connect to the desired virtual conference room.

Flexible Conference Profile Administration

SM7000 allows platform managers to setup unlimited number of conference profiles to allow flexibility and high system throughput. In addition, the profiles allow Managed Services support for virtual platform partitioning.

RADIUS Billing Interface

SM7000 supports RADIUS Billing Interface to SysMaster VM2000 Billing Platform. This allows the conference server to support real time billing procedures where as all outbound and inbound conference calls are accounted and billed for. All call billing and routing is done in real-time.

Custom Announcement Procedure

SM7000 supports flexible Language Server setup to allow easy prompt and IVR management in multiple languages. Each customer can define a custom prompt on all conference call levels.

Conference Server

Call Flow

One-Stage Conference Calling

1. Caller dial an 800 number (DID) or connects to SM7000 via VoIP
2. SM7000 accepts the call
3. SM7000 plays Welcome Message
4. SM7000 asks for PIN Number
5. Caller Enters PIN Number
6. Caller is entered into a virtual conference room associated with the DID
7. All callers are now in conference
8. SM7000 sends Radius signals to VM2000 for Billing purposes
9. Conference administrators manage callers and record sessions

Two-Stage Conference Calling

1. Caller dial an 800 number (DID) or connects to SM7000 via VoIP
2. SM7000 accepts the call
3. SM7000 plays Welcome Message
4. SM7000 asks for a Virtual Conference Room Number
5. SM7000 asks for PIN Number
6. Caller Enters PIN Number
7. Caller is entered into a virtual conference room
8. All callers are now in conference
9. SM7000 sends Radius signals to VM2000 for Billing purposes
10. Conference administrators manage callers and record sessions

Language Servers are used to store audio files through which the IVR logic will assemble audio messages, e.g. announcing numbers, text messages and prompts. To this end, a Language Server is pointed to in the IVR Profile. A Language Server actually represents a directory on a remote server (TFTP protocol server) where audio files are stored. The SysMaster gateway can also store locally multiple audio files. Each audio file has a name defined by a short designation of the language as well as a part determining the type of message it holds.

Setup Workflow

1 Specify an IVR Profile of the type

- For One-stage Conference server - create an IVR Profile of type “Conference“
- For Two-stage Conference server - create an IVR Profile of type “Conference/Two Stage”

2 Specify an Inbound profile with the created IVR.

- For One-stage, specify DNIS translation with the extension of the conference room. e.g. S=99922.
- For Two-stage, leave DNIS empty. The room extension should be supplied during the second stage of the dialing.

3 Create a call filter catching the number used to join conference rooms.

- For One-stage access, each room should have its own Call filter to catch and redirect the calls.
- For two-stage conference rooms it is necessary to create at least one Call filter redirecting users to join a Conference room.

Parameters:

Extension Number	Designates the conference room number. Users can participate should use this number to enter the room.
Conference Name	Assigns a name to the conference room. The name is used only internally for system setup.

Conference Type	Specifies the conference type to be applied. Available choices are: ■ **Private** - callers are required to enter password upon conference entrance ■ **Public** - callers are accepted to conference without a password prompt and admin present ■ **Private:Listen-Only** - callers can listen only to conference and password is required for them to join in. ■ **Public: Listen-Only** - callers can listen to conference only and password is not required for them to join in. ■ **Private:Screen** - callers are required to enter password upon conference entrance and admin must be present for them to join the conference room. ■ **Public:Screen** - callers are not required to enter password upon conference entrance, but admin must be present for them to join the conference room.
Max Calls (3-1000)	Defines the maximum number of calls for the room.
Admin PIN	Specifies the administrative password used by administrators when entering the conference room by administrators. The administrative PIN grants additional capabilities to the manage the calling parties participating in the conference room.
Access PIN)	Specifies the password used by calling parties in order to join the conference room.
Monitoring PIN	This PIN allows for specialia access to the conference room. Using it, administrators can join a room as spectators i.e. they only monitor the activity within the room.
Admin Email	Specifies the email that the system uses to send recorded conversations of the conference sessions.
Auto Recording	Activates the recording mode whenever there is at least one calling party in the conference room.
Status Anouncement	Forces an informational announcement about the time the conference session has started as well as the current number of users in it. The announcement is played right before a user joins the room.
Admin Required	If checked, callers cannot start conference but stay on hold, until admin is available.

Music On Hold	Specifies the type of Music On Hold to be played.
Scheduled Events	Specifies scheduled events to be performed.
Auto Dial Numbers	Specifies one or more auto-dial numbers used to faster access to conference room.
Advanced Rule	Specifies the Advanced Rule to be applied to the Call Filter. Advanced Rules allow for flexible enforcement of the call filter based on time or endpoint availability.
Description	Short description (up to 71 characters) about the Conference room.

Managing Conference Rooms

To Add Conference Room

1. From the Navigation tree, select the **Conferencing > Conference Rooms** node.
2. From the Edit Menu select 'Add Conference Room'.
   A dialog box shows up.
3. Fill in the data, and click on the Apply button to enforce modifications.

To Edit Conference Room

1. From the Navigation tree, select the **Conferencing > Conference Rooms** node.
2. From the right pane of the Navigator, select the Conference room to be edited.
3. From the Edit Menu select 'Edit Conference Room'.
   A dialog box shows up.
4. Fill in the data, and click on the Apply button to enforce modifications.

To Delete Conference Room

1. From the Navigation tree, select the **Conferencing > Conference Rooms** node.
2. From the right pane of the Navigator, select the Conference room to be deleted.
3. From the Edit Menu, select the Delete menu item.

Chapter 13 Follow-Me Server

Introduction

Overview

The Follow-me server allows platform administrators to define one phone number that will hunt multiple phone numbers in specific order to try to locate the follow-me subscriber. If located, the subscribed may pick up the phone and accept or reject the call based on his caller id or calling party name preferences. If the subscriber is not located, the system will default to his voice mailbox. The service will guarantee global, international roaming and 100% availability for all subscribers.

Features

- Multi-Number Hunting and Global Roaming
- Long-Distance and International Number Support
- H323, SIP, PSTN Least Cost Routing
- Secure Caller Authentication
- Email Notification
- Voice Mail Failover
- Anonymous Number Support
- Dynamic Phone Number Change
- Web User Administration

Follow-Me Server

Call Flow

One-Stage Follow-Me Calling

1. Caller dials a DID number or connects to SM7000 via VoIP
2. SM 7000 accepts the call
3. SM 7000 plays a subscriber message
4. SM 7000 hunts the subscriber and rings up his phone
5. Subscriber picks up the phone
6. SM 7000 connects both parties
7. Conference administrators manage callers and record sessions

Two-Stage Follow-Me Calling

1. Caller dials a DID number or connects to SM7000 via VoIP
2. SM 7000 accepts the call
3. SM 7000 ask the caller to provide his name
4. SM 7000 plays a subscriber message
5. SM 7000 hunts the subscriber and rings up his phone
6. Subscriber picks up the phone
7. SM 7000 displays his ANI and plays the name of the caller to the subscriber
8. Subscriber accepts of rejects the call
9. SM 7000 connects both parties

Language Servers are used to store audio files through which the IVR logic will assemble audio messages, e.g. announcing numbers, text messages and prompts. To this end, a Language Server is pointed to in the IVR Profile. A Language Server actually represents a directory on a remote server (TFTP protocol server) where audio files are stored. The SysMaster gateway can also store locally multiple audio files. Each audio file has a name defined by a short designation of the language as well as a part determining the type of message it holds.

Setup Workflow

1. Specify an IVR Profile of the type

   - For One-stage Conference server - create an IVR Profile of type “Conference“
   - For Two-stage Conference server - create an IVR Profile of type “Conference/Two Stage”

2. Specify an Inbound profile with the created IVR.

   - For One-stage, specify DNIS translation with the extension of the conference room. e.g. S=99922.
   - For Two-stage, leave DNIS empty. The room extension should be supplied during the second stage of the dialing.

3. Create a call filter catching the number used to join conference rooms.

   - For One-stage access, each room should have its own Call filter to catch and redirect the calls.
   - For two-stage conference rooms it is necessary to create at least one Call filter redirecting users to join a Conference room.

Parameters:

Extension	The extension number at which the calling party connects to the Follow-Me functionality of the destination party.

Password	Specifies the password through which the user manages his/her Follow-me settings. The management is performed through a phone.
Verify Password	Verifies the password.
Enable Follow-Me	If checked, the Follow-Me profile will be enabled. If unchecked the Follow-Me profile will be inactive.
Enable Call Screen	If checked, the Call Screen functionality is enabled. The Call Screen requires the calling party to leave a message about himself/herself. This allows the called party to see the who is calling and to further decide whether to accept or reject the call.
Follow-Me Numbers	Specifies a comma-separated list of phone numbers to be sequentially called (hunted).
Voice Mail Number	Specifies the fall-back Voice Mail number to which a Voice Mail message can be left. The Voice Mail functionality is engaged only if a number is provided.
Connect Timeout (sec)	Specifies the time interval between attempting the next number specified in the Follow-Me number list.
Description	Provides a short description for the Follow-Me profile.

Managing Follow-Me Profiles

To Add Follow-Me Profile

1. From the Navigation tree, select the **Follow Me > Follow Me Profile** node.
2. From the Edit Menu select 'Add Follow Me Profile'
   A dialog box shows up.
3. Fill in the data, and click on the Apply button to enforce the modifications.

To Edit Follow-Me Profile

1. From the Navigation tree, select the **Follow Me > Follow Me Profile** node.
2. From the right pane of the Navigator, select the Follow Me Profile to be edited.
3. From the Edit Menu select 'Edit Follow Me Profile'.
   A dialog box shows up.
4. Fill in the data, and click on the Apply button to enforce modifications.

To Delete Follow-Me Profile

1. From the Navigation tree, select the **Follow Me > Follow Me Profile** node.
2. From the right pane of the Navigator, select the Follow Me Profile to be deleted.
3. From the Edit Menu, select the Delete menu item.

Chapter 14 System Monitoring

Calls Overview

This chapter describes SysMaster Calls module and tells you how to view and understand information regarding system processes and calls generated by the system. Calls information is provided for administrative purposes only.

The following call information could be viewed:

- Current Calls
- Recent Calls
- Gateway Monitor

Current Calls

Current Calls display information about all calls in process. You can reach the Current Calls by navigating to **Calls** node to expend it and highlighting **Current Calls**. Once displayed system administrators could view all details associated with a call in progress.

The information displayed in the Current Call screen is not automatically updated. All data is only relevant up to the point of opening the current call screen. In case that call information is continuously monitored, the Refresh Page button should be pressed for the most current information to be displayed.

Recent Calls

Recent Calls display all calls that have been terminated and already billed by the system. You can access Recent Calls information by:

1. In the Navigator, click on the **Calls** node to expand it.
2. Highlight the **Recent Calls** node
3. A screen showing all information relevant to recent calls would be displayed to the left side of the navigation tree.

Recent Calls parameters are

Session ID	Specifies the session ID of the call.
Callback ID	Specifies the delta charge for the Initial Charge in US cents. The Init Charge specifies the amount that the user will be charged for the communication service during the Init Time.
Start Time	Specifies the time when the call was placed.
End Time	Specifies the time when the call was ended.
Session Time	Specifies the duration of the call in minutes
Called Stations	Specifies the destination number dialed when placing the call.
Calling Station	Specifies the calling number of the placed call.
Local IP Address	Specifies the IP address that was used for VoIP communications
Remote IP Address	Specifies the IP address of the destination enpoint used in VoIP communications.
Gatekeeper IP Address	Specifies the IP address of the gatekeeper used in routing of the finished call
Disconnect Cause	Specifies the disconnect cause or the reason for call termination
PBX Group	Specifies the PBX Group the call belongs to. PBX groups are associated with inbound profiles.
Codec	Specifies the codec used in routing of the call.
Protocol	Specifies the type of protocol used in routing of the call.
Jitter	Specifies the amount of jitter associated with the call. Jitter is used to buffer incoming packets to allow for high latency networks to support VoIP communication. The recommended value for jitter is between 50 and 300 ms.
Latency	Specifies the latency of the call as measured by the gateway in milliseconds.
Bytes IN	Specifies the size of the incoming traffic in bytes.
Bytes OUT	Specifies the size of the outgoing traffic in bytes.
Packets IN	Specifies the size of the incoming traffic in packets.
Packets OUT	Specifies the size of the outgoing traffic in packets.
Voice Quality	Designates the level of voice quality.

IVR type	Specifies the type of the IVR profile used in routing of the finished call.
IVR Profile	Specifies the IVR Profile used in the routing of the finished call. IVR Profiles are used by PBX Groups.
Route ID	Specifies the Route ID of the finished call.
Provider	Designates the name of the provider associated with routing the finished call.
RADIUS Group	Designated the RADIUS group used in routing of the finished call.
PIN	Specifies the PIN number (if any) associated with the finished call.
Credit Time	Specifies the credit time for the finished call.
Credit Amount	Specifies the amount of credit used up for the duration of the call.
Call Type	Specifies the type of the recent call.

Gateway Monitor

Gateway Monitor provides visual representation of gateway parameters. Gateway parameters are viewed according to the IP address of the gateway and not its H.323 ID. The report shows the gateway ports, today calls, number of connections, latency, utilization and ASR.

To generate a gateway history report:

1. In the Navigator, click on the **Calls** node to expand it.
2. Highlight the **Gateway Monitor** node.
   A graphical gateway monitor interface would be displayed.

System administrators could export or print gateway history. For you convenience, prior to printing the report, please ensure that the printer paper layout is set to Landscape. To get the full benefit of history reports, we recommend you print/export them on regular basis and keep them for future references.

Printing Gateway Monitor History

This section outlines how to print Gateway Monitor History.

Print gateway monitor history as follows:

1. In the Navigator, click on the **Calls** node to expand it.
2. Highlight the **Gateway Monitor** node.
   A graphical gateway monitor interface would be displayed.

3 Click on File | Print to print the report

Exporting Gateway Monitor History

This section outlines how to export Gateway Monitor History.

Export gateway monitor history as follows:

1 In the Navigator, click on the **Calls** node to expand it.

2 Highlight the **Gateway Monitor** node.
A graphical gateway monitor interface would be displayed.

3 Click on File | Export to export the report

Chapter 15 Appendix A

SysMaster Gateway Command Line Interface

The SysMaster Gateway provides a CLI interface for managing and viewing the gateway parameters and activity. Access to the gateway is possible through an SSH client. The initial username with which the gateway comes shipped is “admin“ with no password set. You are advised to set a password before the gateway is put in production environment. Once logged in, the system allows you to execute one of the listed commands:

cpu	getroute	reboot
database	halt	si
date	hostname	span
dnslookup	ip	spans
domainname	passwd	traceroute
exit	ping	voip

All configuration data is contained in 'Files'. Each file actually represents a configuration variable. There are also directories representing a group of files and/or other directories. All directories are organized in a tree-like structure. There two types of directories: regular directories and lists. Regular directories can contain files, other directories and lists Lists represent an ordered lists of elements each of which has a set of variables attached to it. The base directory is a parent to all other directories. It is called root directory. The Command Line Interface allows you to navigate throughout the file system as well as perform basic configuration and administrative tasks. When working with file names, the CLI always needs to know the fully specified name of a file. A fully specified file name includes a path name plus the name of the file itself. The path indicates the directory in which the file is located. Path names can include alphanumerical characters, space, '_', '-' and the special symbols '/', '.', '..'.

- The symbol '/' represents the root directory (the parent directory of all directories).
- The symbol '.' represents the current directory.
- The symbol '..' represents the directory one level higher than the current directory.

If no path is provided or only a relative path name is provided, the CLI takes into account the current directory to construct the fully specified file name. Fully specified file name shows the location of a file in regards to the root directory. The current directory holds a reference to the directory from which the CLI should construct all fully specified file names. In other words, the current directory provides the directory context for the CLI. Paths can be absolute or relative. Absolute path names use the root directory as a reference. The relative path names use the current directory as a reference.

[examples]:

- Absolute path name:

  /Edit Cfg/Host Setup/Telnet Access

- Relative path name:

If the current directory is /Edit Cfg/Host Setup/Web Access

then ../Telnet Access specifies the directory:

/Edit Cfg/Host Setup/Telnet Access

- Fully specified file name:

/Edit Cfg/Host Setup/Web Access/var1

The SysMaster CLI also supports TAB based syntax, file/directory name and value completion. When using a command on a file(s), a directory(s) or a list(s), the CLI can prompt you for the available names or values to use. To that end, you need to enter the first one or more letters of the file/directory name and then press the TAB key to browse through the available file/directory names or simply after the command press the TAB to list all available options.

cpu

This command reports information about CPU utilization. The first row gives average values since the last reboot. Additional rows give information on a sampling period of length delay.

[usage]:

```
cpu [delay]
```

[options]:

`delay`
Displays the delay in seconds between updates.

database

This command is used for database management. Managing includes dump, reset and restore. For every action a confirmation with 'yes' is required.

[usage]:

```
database [OPTIONS]
```

[options]:

`-dump`
Stores a copy of the database. The copy may be used for restoring of damaged database.

`-reset`
Reverts the database to its initial state (no data remains).

`-restore`
Recovers the database from existing copy.

date

Display or set the system date and time

[usage]:

```
date [MM-DD-YYYY hh:mm:ss]
```

[options]:

-MM
Specifies the month. Allowed values are from 01 to 12

-DD
Specifies the day. Allowed values are from 01 to 31

-YYYY
Specified the year. Allowed values are from 2000 to 9999

-hh
Specifies the day hour. Allowed values are from 00 to 23

-mm
Specifies the hour minutes. Allowed values are from 00-59

-ss
Specifies the minute seconds. Allowed values are from 00-59

dnslookup

Performs a DNS lookup or reverse DNS lookup operation depending on the host parameter. When the host parameter is a valid DNS name, the command performs a DNS lookup by querying a default (unless explicitly specified) DNS server to resolve the host name to an IP address. When the host parameter is an IP address, the command performs a reverse DNS lookup, resolving to a host name.

[usage]:

```
dnslookup [-t TYPE] host [server]
```

[options]:

-t TYPE
Specifies the type of records the command queries for. They can be A, NS, CNAME, PTR, MX

-host
Specifies the host name/IP address to be resolved

-server
Specifies the DNS server to be queried. If omitted, the default DNS server is queried.

domainname

Show or set the system domain name. When called without argument the command displays the current domain name. When called with one argument the command sets the domain name.

[usage]:

```
domainname [name]
```

exit

Exits the CLI utility.

[usage]:

```
exit
```

getroute

Displays a route which SysMaster uses for a specified pair of local and remote IP addresses or a pair of a destination IP address and a network device.

[usage]:

```
getroute [-f FROM] [-t TO] [-i INIF] [-o OUTIF]
```

[options]:

`-f FROM`
Specifies a local IP address

`-t TO`
Specifies a destination IP address

`-i INIF`
Specifies the input network device. It can be NA-n (n=1,..,8), BR-n (n=1,..,4), WAN-n (n=1,2), IPS-n (n=1,..,4), PPP-n.

`-o OUTIF`
Specifies the output network device. It can be NA-n (n=1,..,8), BR-n (n=1,..,4), WAN-n (n=1,2), IPS-n (n=1,..,4), PPP-n.

[example]:

```
getroute -t 10.0.0.1 -f 192.168.0.1

getroute -t 10.0.0.1 -o NA-1
```

halt

Halts the system. Requires confirmation from the user. By selecting 'y' you will confirm the halt action.

[usage]:

```
halt
```

help

[usage]:

```
help <command>
```

Display help information about a command, directories and files.

hostname

Show or set the system host name. When called without argument the command displays the current host name. When called with one argument the command sets the sets the hostname.

[usage]:

```
hostname [name]
```

ip

Display, add or delete local IP addresses or routes.

[usage]:

```
ip [OPTIONS]
```

[options]:

```
-address [add|edit|del|show] [IP address[/nbm]] dev DEVNAME [TYPE]
```

```
- nbm
```
Netbits (default 32) or netmask

```
-DEVNAME
```
eth0, eth1, eth2, eth3

```
-TYPE
```
public (default) or private

-route [add|edit|del|show] [IP1 address[/nbm]] gw IP2 dev DEVNAME [status]

```
- nbm
```
Netbits (default 32) or netmask

`-IP1`
Destination IP address

`-IP2`
Gateway IP Address

`-DEVNAME`
eth0, eth1, eth2, eth3

`-status`
Enabled (default), disabled

[examples]:

```
ip address add 192.168.0.99/32 dev eth2 private

ip address edit 192.168.0.99/24 dev eth3 public

ip address show

ip address del 192.168.0.67/24 dev eth3

ip route add 192.168.0.55/24 gw 192.168.0.5 dev eth1

ip route edit 192.168.0.55/24 gw 192.168.0.5 dev eth1 disabled

ip route show

ip route del 192.168.0.55/24 gw 192.168.0.5 dev eth1
```

passwd

Changes the admin password

[usage]:

```
passwd
```

ping

Sends ECHO ICMP packets to a specified host. This command is used to determine whether certain host availability on the network.

[usage]:

ping [-f SRC] [-c COUNT] [-i INTERVAL] host

[options]:

`-host`
Specifies the destination host name to be pinged. It can be a valid domain name or an IP address.

`-f SRC`
Specifies the interface from which the packets are sent

`-c COUNT`
Specifies the number of packets to be sent

`-i INTERVAL`
Specifies the interval at which packets will be sent.

reboot

Reboots the system. Requires confirmation from the user. By selecting 'y' you will confirm the reboot action.

[usage]:

```
reboot
```

si

Displays system info about the SysMaster device.

[usage]:

```
si
```

span

Shows available T1/E1 span

[usage]:

```
span [COMMAND] [PARAMETERS]
```

[options]

`COMMAND: monitor, show, state`

`PARAMETERS: <span number>, <time interval>` in seconds

`-monitor <span number> [<time_interval>]`
Monitors the T1/E1 Span channels information. The information is displayed in interval specified by time interval option until Ctrl+C is pressed. If not specified, the default time interval is 1 second.

`-show <span number>`
Shows the information for the specified T1/E1 Span.

`-state monitor <span number> [<time_interval>]`
Monitors the span state information. The information is displayed in interval specified by time_interval option until Ctrl+C is pressed. If not specified, the default time interval is 1 second.

`-state show <span number>`
Shows the span state information for the specified T1/E1 Span.

spans

Shows available T1/E1 Spans.

[usage]:

```
spans
```

traceroute

Discovers the route of a packet in its way to a destination host. The command uses ICMP echo packets with specified TTL (Time To Live) values to the destination host. The TTL value of the packet is decremented by one each time it is forwarded through a router (a hop).

[usage]:

```
traceroute [-f SRC] [-t MAXTTL] [-r] host
```

[options]:

`-f SRC`
Specifies the interface from which the packets are sent.

`-t MAXTTL`
Specifies the number of hops to trace.

`-r`
Specifies that the command will resolve addresses.

`-host`
Specifies the destination host name to be traced. It can be a valid domain name or an IP address.

voip

[usage]:

```
voip debug [COMMAND] session [SESSION_ID] request   [REQUEST_ID]
system [SYSTEM]\var=value
```

[options]

```
COMMAND:
- start, stop, list

SESSION_ID:
- number, 1-9

SYSTEM:
-all, h323gw, h323proxy, sipgw, ivr, callback
```

`var=value`
Specifies system specific parameters

`-debug`
Debug calls

`-drop`
Drop the selected call

`-show`
Show info